りそな中小企業振興財団
経営講演会

2020年11月30日

中小企業のサイバーセキュリティ

東京電機大学
顧問・客員教授
佐々木良一
r.sasaki@mail.dendai.ac.jp

イントロダクション

自己紹介：**佐々木良一**　（東京電機大学客員教授）

1971年ー2001年　日立製作所。1984年より情報セキュリティなどの研究に従事

2001年ー2018年3月　東京電機大学未来科学部教授

2018年ー2020年3月　総合研究所　特命教授

サイバーセキュリティ研究所長

日本セキュリティマネジメント学会会長
デジタルフォレンジック研究会会長
内閣官房サイバーセキュリティ補佐官
などを歴任

目次

三菱電機にサイバー攻撃 防衛などの情報流出か

- 大手総合電機メーカーの三菱電機が大規模なサイバー攻撃を受け、機密性の高い防衛関連、電力や鉄道といった重要な社会インフラ関連など官民の取引先に関する情報が広く流出した恐れがあることがわかった。
- 本社や主要拠点のパソコンやサーバーが多数の不正なアクセスを受けたことが社内調査で判明した。
- 同社は不正アクセスの手口などから、防衛関連の機密情報を主に狙う中国系のサイバー攻撃集団「Tick（ティック）」が関与した可能性があるとみている。

2020年1月
https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html

ランサムウエアの被害

カプコン サイバー攻撃 金銭要求の「ランサムウェア」

2020年11月12日 18時19分　IT・ネット

https://www3.nhk.or.jp/news/html/20201112/k10012708311000.html

中小企業のセキュリティアンケート方法

- 実施期間：2019年11月12日(火)～11月15日(金)
- 調査方法：インターネット調査
- 回答数　：中小企業の経営者・役員825人

日本損保保険協会の調査

https://www.sonpo.or.jp/news/release/2019/2001_02.html

中小企業のセキュリティアンケート（1）

中小企業の約2割はサイバー攻撃の被害経験あり。

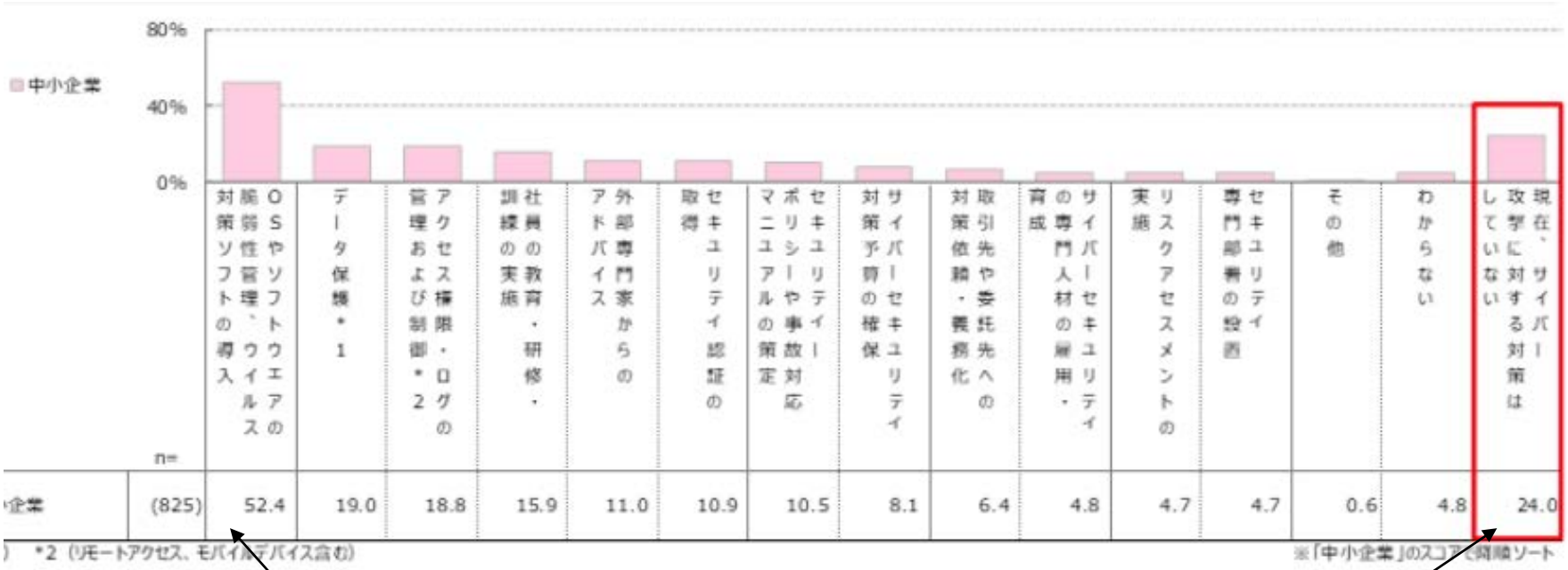
被害額が数千万円を超えるものも。

日本損保保険協会の調査

https://www.sonpo.or.jp/news/release/2019/2001_02.html

中小企業のセキュリティアンケート（2）

中小企業の4社に1社は、今もなおサイバー攻撃への対策をしていない



OSやソフトの脆弱性対策・ウイルス対策ソフト（52.4%）

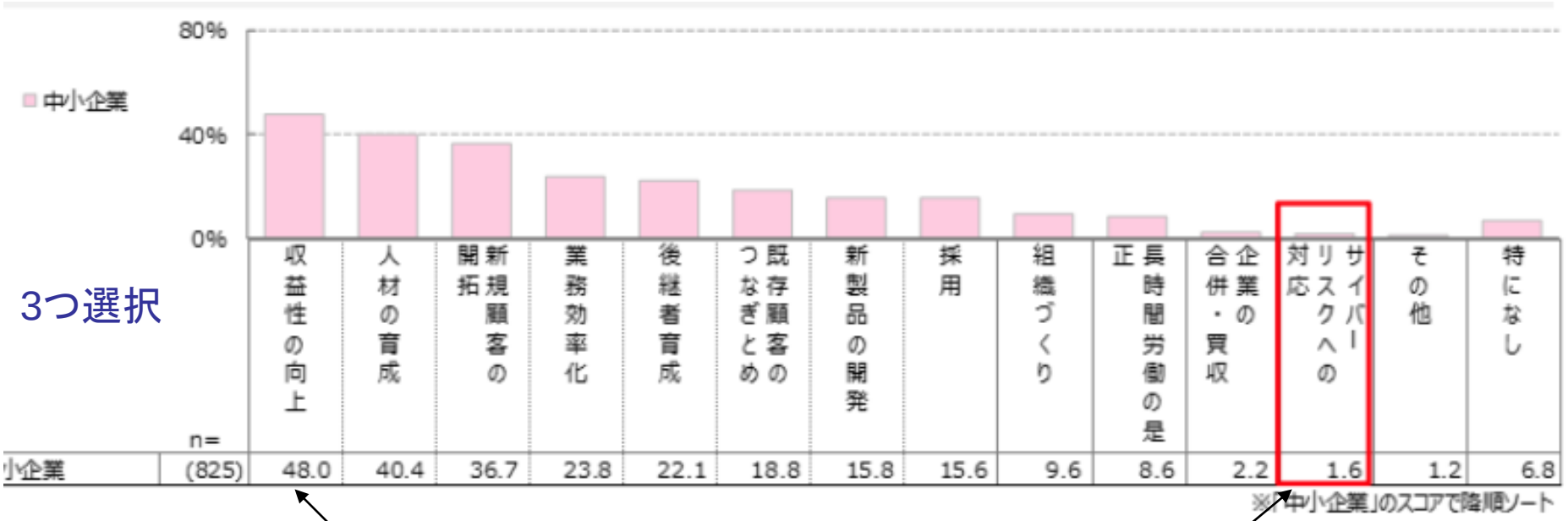
対策はしていない（24.0%）

日本損保保険協会の調査

https://www.sonpo.or.jp/news/release/2019/2001_02.html

中小企業のセキュリティアンケート（3）

サイバー攻撃への対策は、他の経営課題より優先度が低い



収益性の向上
（48.0ポイント）

サイバーリスクへの
対応（1.6ポイント）

日本損保保険協会の調査

https://www.sonpo.or.jp/news/release/2019/2001_02.html

中小企業のセキュリティアンケート（4）

中小企業の約2割はサイバー攻撃の被害経験あり。

被害額が数千万円を超えるものも。

サイバー攻撃の状況とセキュリティ対策を紹介

日本損保保険協会の調査

https://www.sonpo.or.jp/news/release/2019/2001_02.html

目次

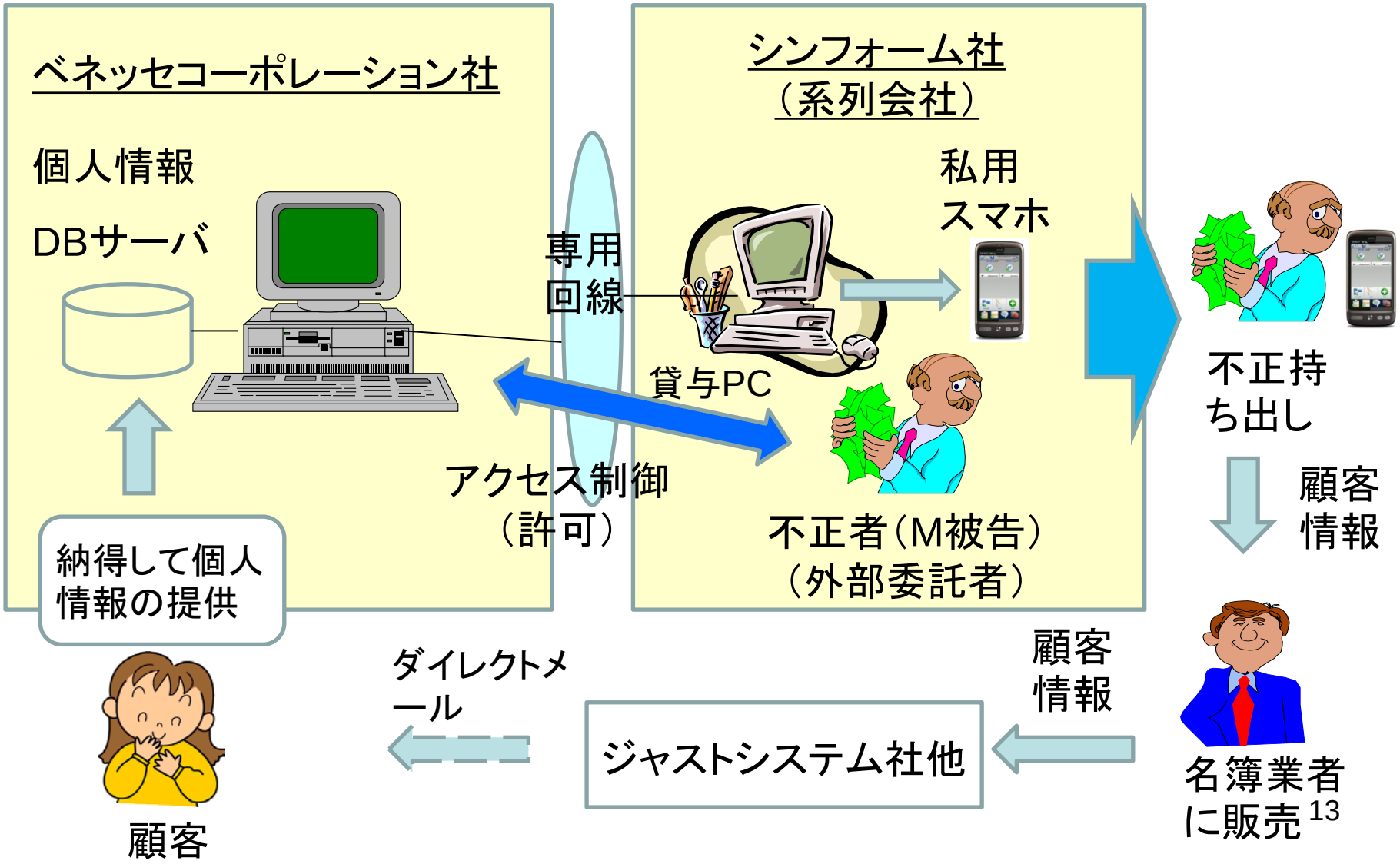
攻撃者と攻撃方法の分類

1．部外者
（a）クラッカー
（b）スパイ
（c）テロリスト
（d）犯罪者等
2．部内者
（a） 従業員
（b）アルバイト等

直接的攻撃
　コンピュータを直接的に操作し、不正アクセスを行いネットワーク上やファイル内のデータを攻撃

間接的攻撃
　ソフトウエアをコンピュータに送り込む事によりファイルなどを攻撃
→ ウイルス

データの持ち出し方法


ベネッセコーポレーション社
個人情報
DBサーバ
専用
回線
シンフォーム社
（系列会社）
私用
スマホ
貸与PC
アクセス制御
（許可）
不正者（M被告）
（外部委託者）
不正持
ち出し
顧客
情報
納得して個人
情報の提供
顧客
ダイレクトメ
ール
顧客
情報
ジャストシステム社他
名簿業者
に販売

ベネッセが実施していた主な対策

- クライアントPCのチェンロック
- 執務室への入退室管理（許可証、監視カメラ設置）
- クライアントPCのネットワーク接続の操作ログ
- クライアントPCのパスワードの定期的変更
- 不要なソフトのインストールの制御
- 不要な外部サービスへのアクセス制御
- セキュリティ教育

（以上、事故調査報告書より）

- その他、USBストレージの利用制限など

ベネッセはプライバシーマークを取得していた

個人情報漏えいによる発生費用

①謝罪広告の掲載
②会見の設定
③おわび状の作成・送付
④顧客への補償
⑤顧客対応コールセンターの設置
⑥応急措置のためのシステム改修
⑦原因究明と本格的な対策の実施
⑧セキュリティー専門家などコンサルティングの実施
⑨サイト停止期間の売り上げ機会損失
⑩社会的信用失墜や企業イメージの低下に伴う経営上の損失
⑪株価の下落による資産の減少
⑫敗訴による損害賠償　など

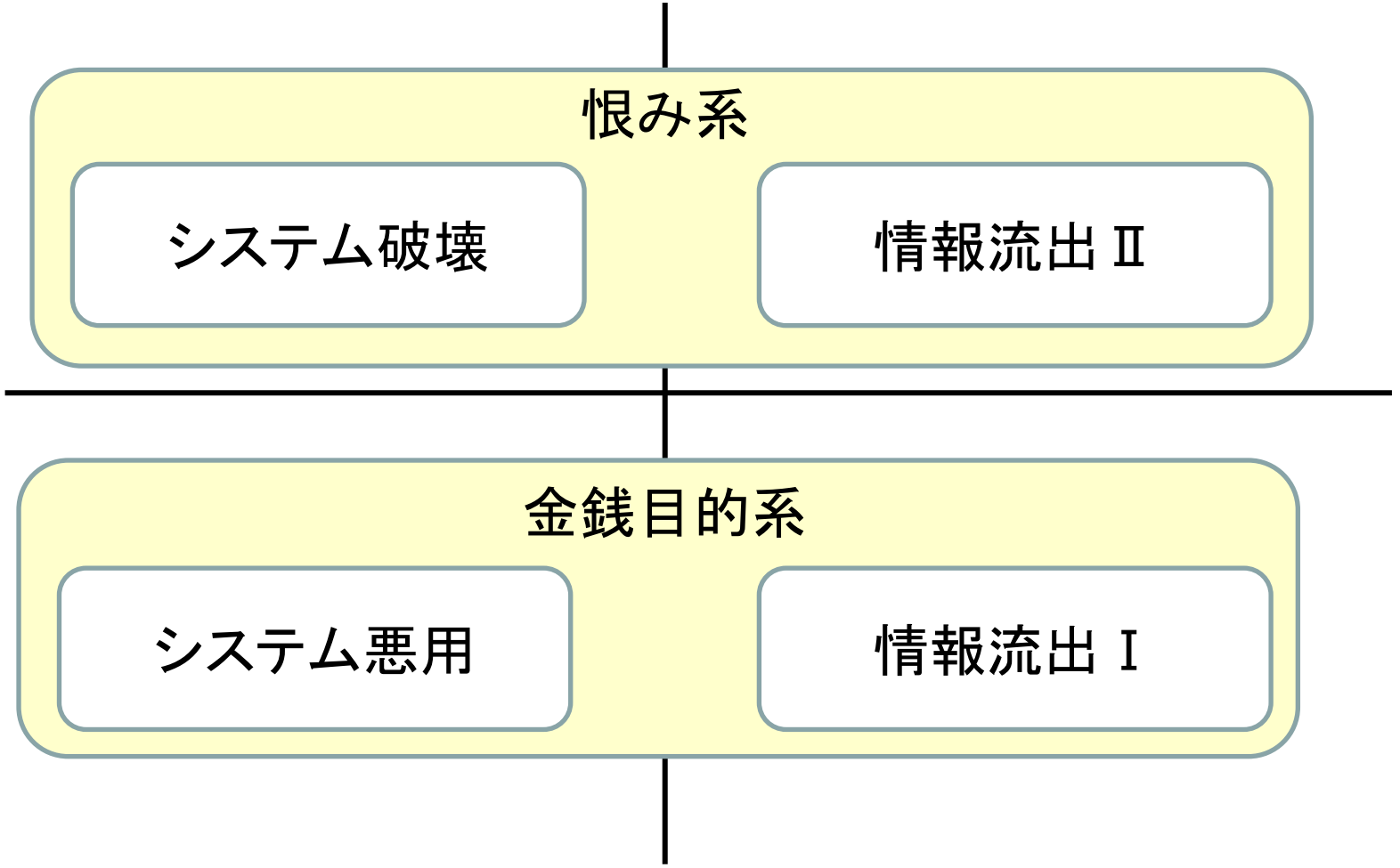
発生費用予測値
数百億円

内部不正を働く動機

No	内容	割合
1	不当だと思う解雇通告を受けた	34．2%
2	給与や賞与に不満がある	23．2%
3	社内の人事評価に不満がある	22．7%
4	職場で頻繁にルール違反が繰り返されている	20．8%
5	システム管理がずさんで顧客情報を簡単に持ち出せることを知っている	20．1%

情報セキュリティ白書2013　p124

内部犯罪者の類型論



法政大学　越智啓太教授　JSSM第27回学術講演会資料を参考に作成

IPA提案内部不正防止対策例

特に重要な情報が保管されているファイルやデータベースについては、以下のような対策をとることで、情報漏えいリスクを低減する必要があります。これらの内容は、IPA「組織における内部不正防止ガイドライン」にわかりやすく記載されています。

① 重要な情報であることを明確にし、適切なアクセス権限を付与すること

② 重要情報の持ち出し・可搬媒体等の持ち込みの監視

③ 定期的な操作履歴の監視・監査

http://www.ipa.go.jp/security/announce/20140710-insider.html

攻撃者と攻撃方法の分類

1．部外者
（a）クラッカー
（b）スパイ
（c）テロリスト
（d）犯罪者等
2．部内者
（a） 従業員
（b）アルバイト等

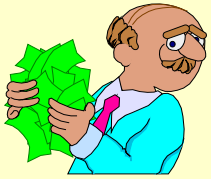
直接的攻撃

コンピュータを直接的に操作し、不正アクセスを行いネットワーク上やファイル内のデータを攻撃

間接的攻撃

ソフトウエアをコンピュータに送り込む事によりファイルなどを攻撃
→ ウイルス

広義のコンピュータウイルスの種類



不正プログラム

- 増殖する（プログラムの機能を利用し侵入）
  - 単独のプログラム
    - コンピュータワーム
  - 他プログラムと合体
    - 狭義のコンピュータウイルス（実行ファイル感染型、マクロ感染型）
- 増殖しない（人をだまして侵入）
  - トロイの木馬

感染形態に着目した分類
もっと広い概念にマルウエアというものがある

Malwareとして扱うもの

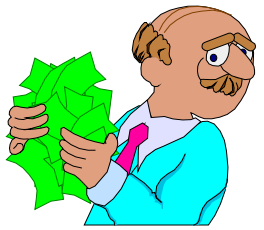
1. ワーム
2. 狭義のウイルス
3. トロイの木馬

＜広義のウイルス＞

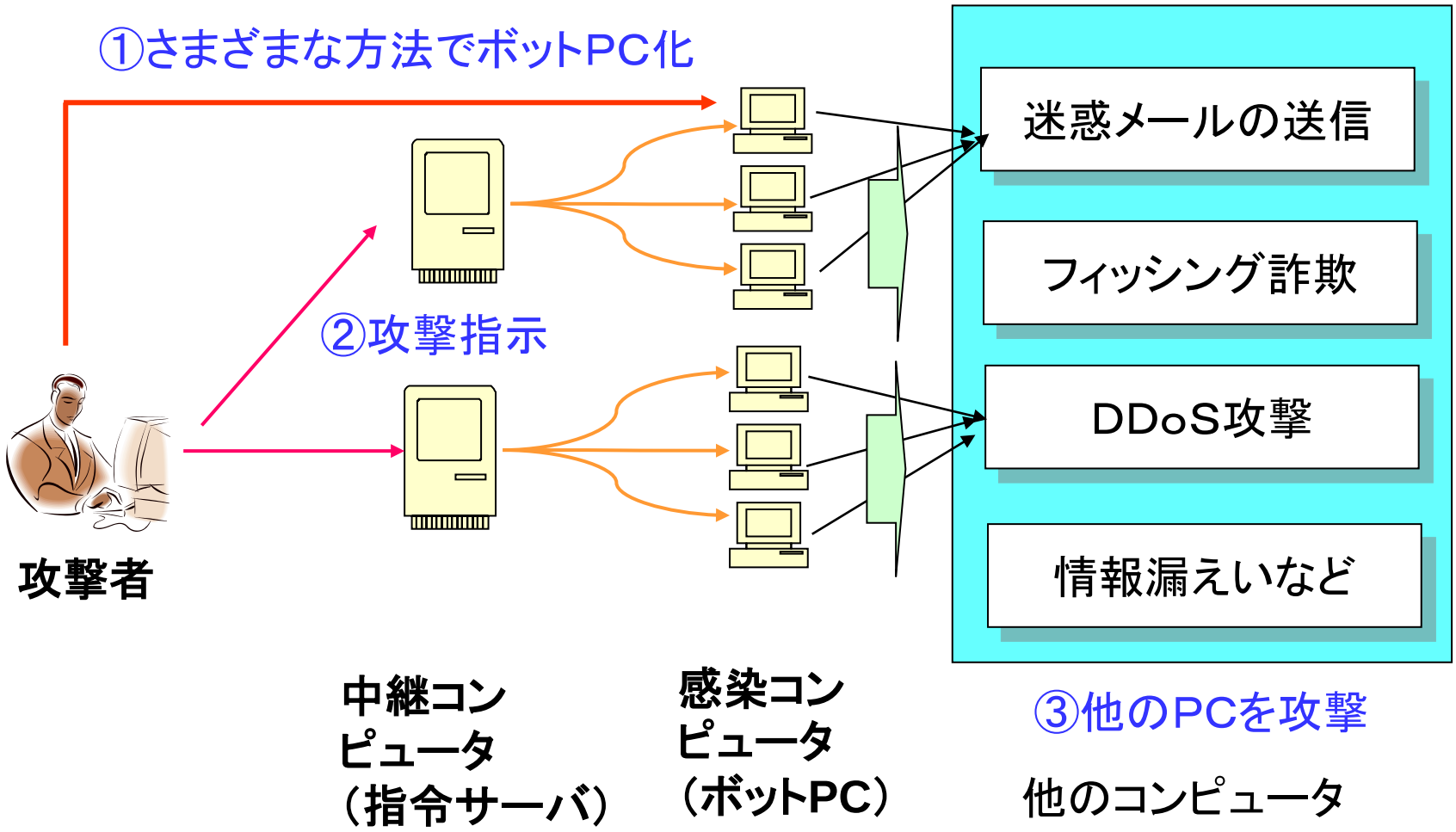
感染形態に着目した分類

4. ボットネット　攻撃システムに着目した分類
5. スパイウエア
6. ランサムウエア
（7. Phishingツール）

目的に着目した分類



ボットネットの概要


①さまざまな方法でボットPC化
②攻撃指示
攻撃者
迷惑メールの送信
フィッシング詐欺
DDoS攻撃
情報漏えいなど
中継コンピュータ（指令サーバ）
感染コンピュータ（ボットPC）
③他のPCを攻撃
他のコンピュータ

Malwareとして扱うもの

1. ワーム
2. 狭義のウイルス
3. トロイの木馬

＜広義のウイルス＞

感染形態に着目した分類

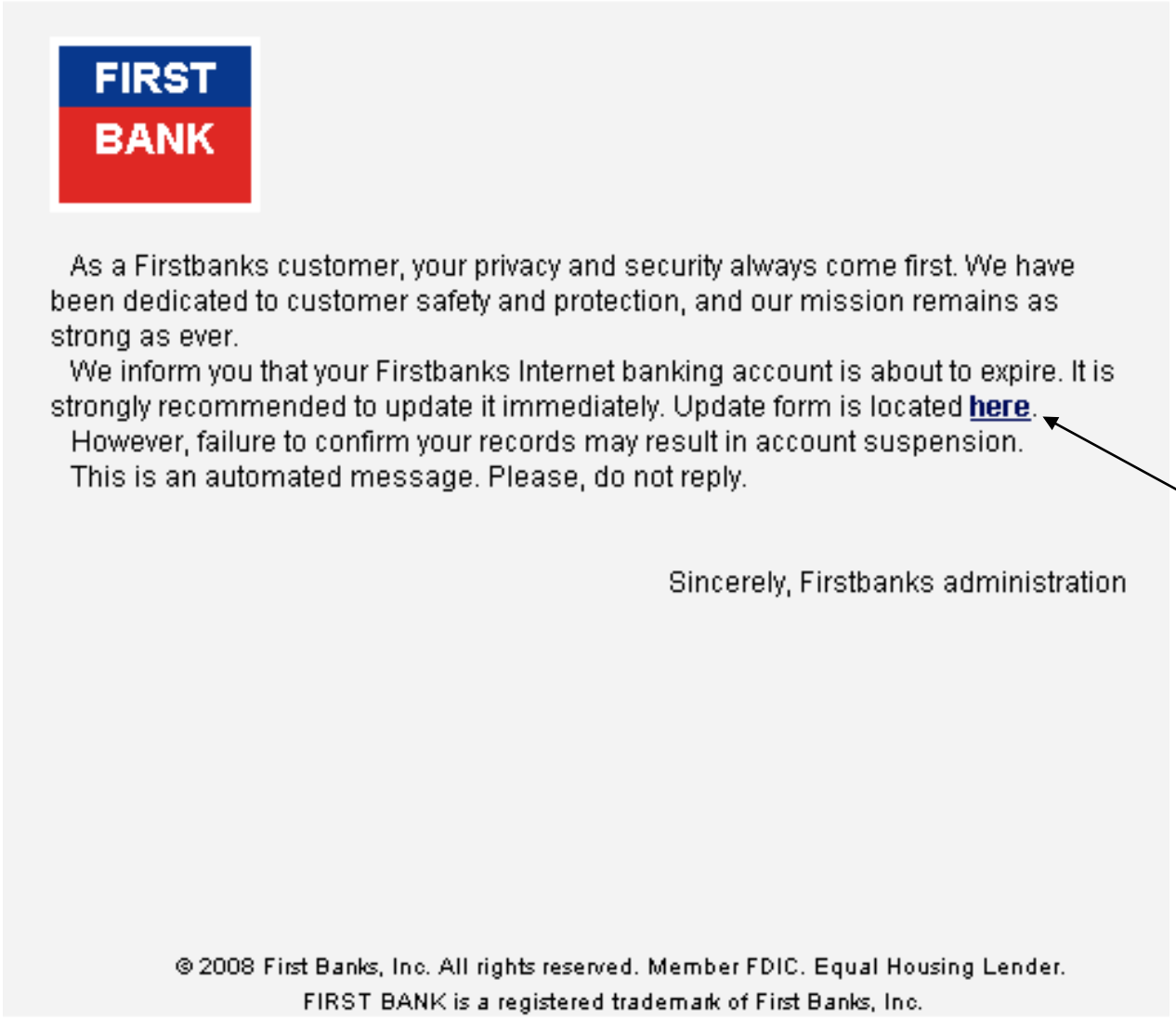
4. ボットネット

攻撃システムに着目した分類

5. スパイウエア
6. ランサムウエア
（7. Phishingツール）

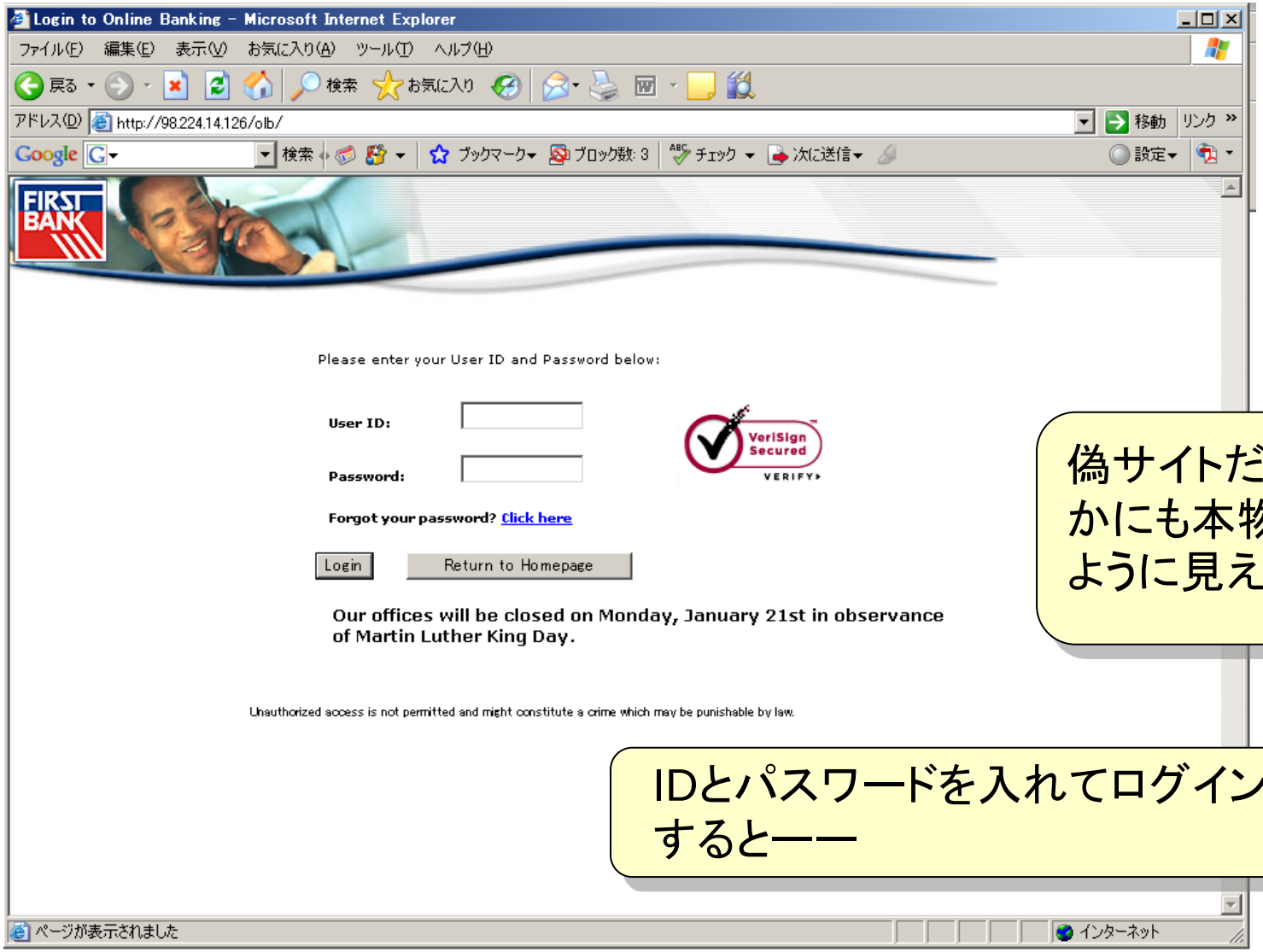
目的に着目した分類

フィッシングメールの一例



早急に対応するためここをクリックせよといっている。

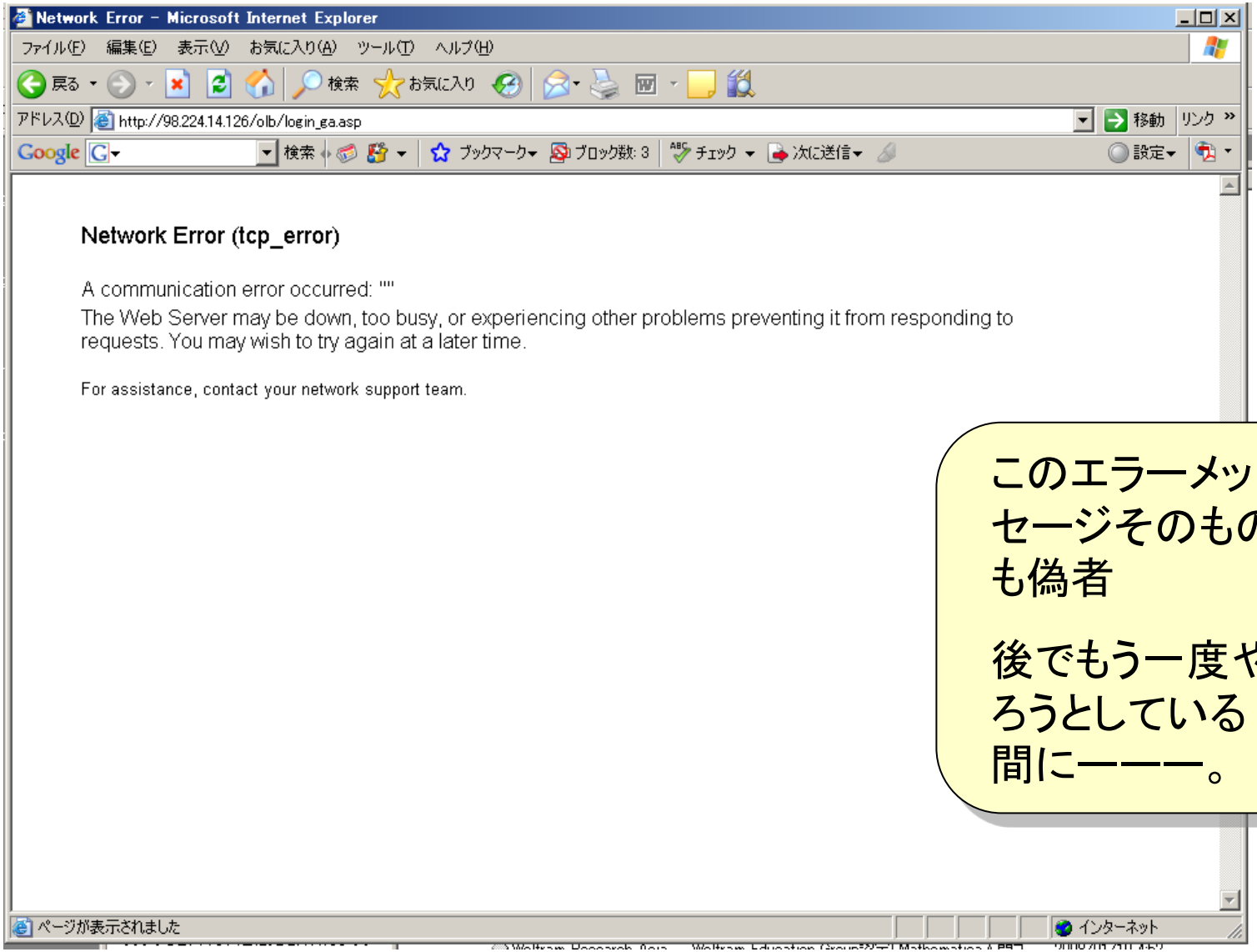
フィッシングサイトの一例



偽サイトだがいかにも本物のように見える。

IDとパスワードを入れてログインすると――

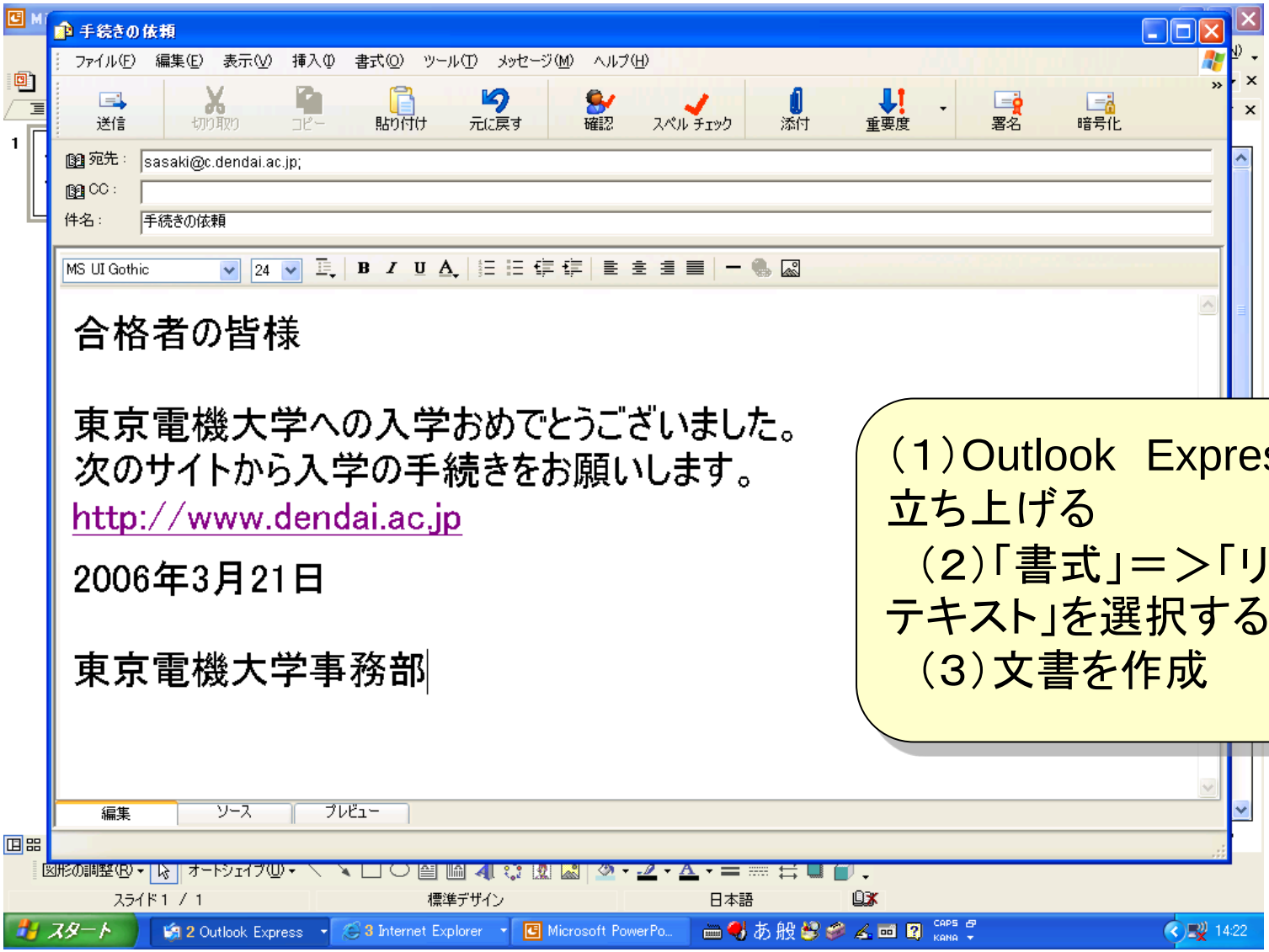
ID・パスワード入力後の画面



このエラーメッセージそのものも偽者

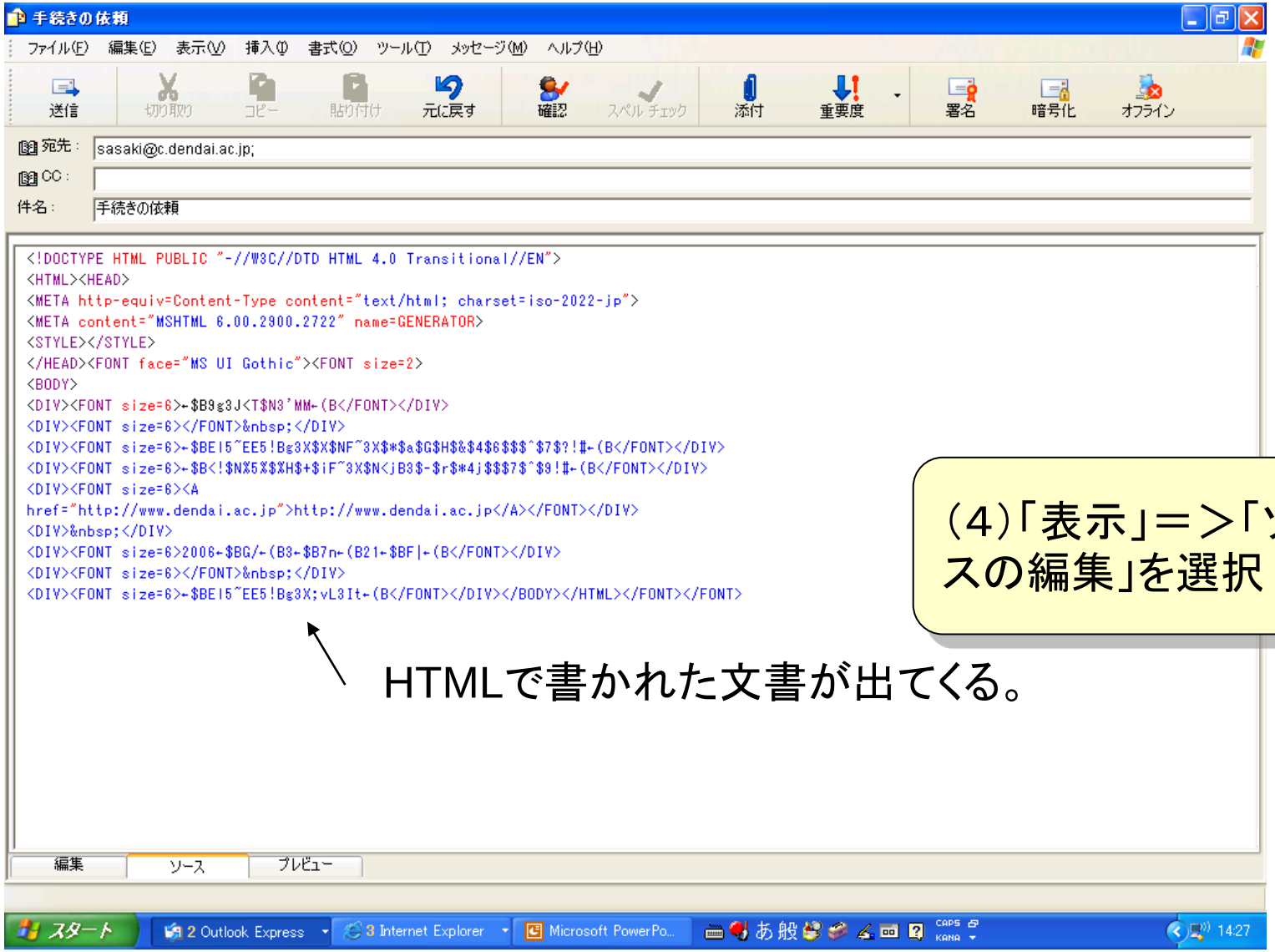
後でもう一度やろうとしている間にーーーー。

フィッシングメールの一例



（1）Outlook Expressを立ち上げる
（2）「書式」＝＞「リッチテキスト」を選択する
（3）文書を作成

フィッシングメールのソースプログラム



(4)「表示」＝＞「ソースの編集」を選択

HTMLで書かれた文書が出てくる。

変更の例

飛び先

表示部

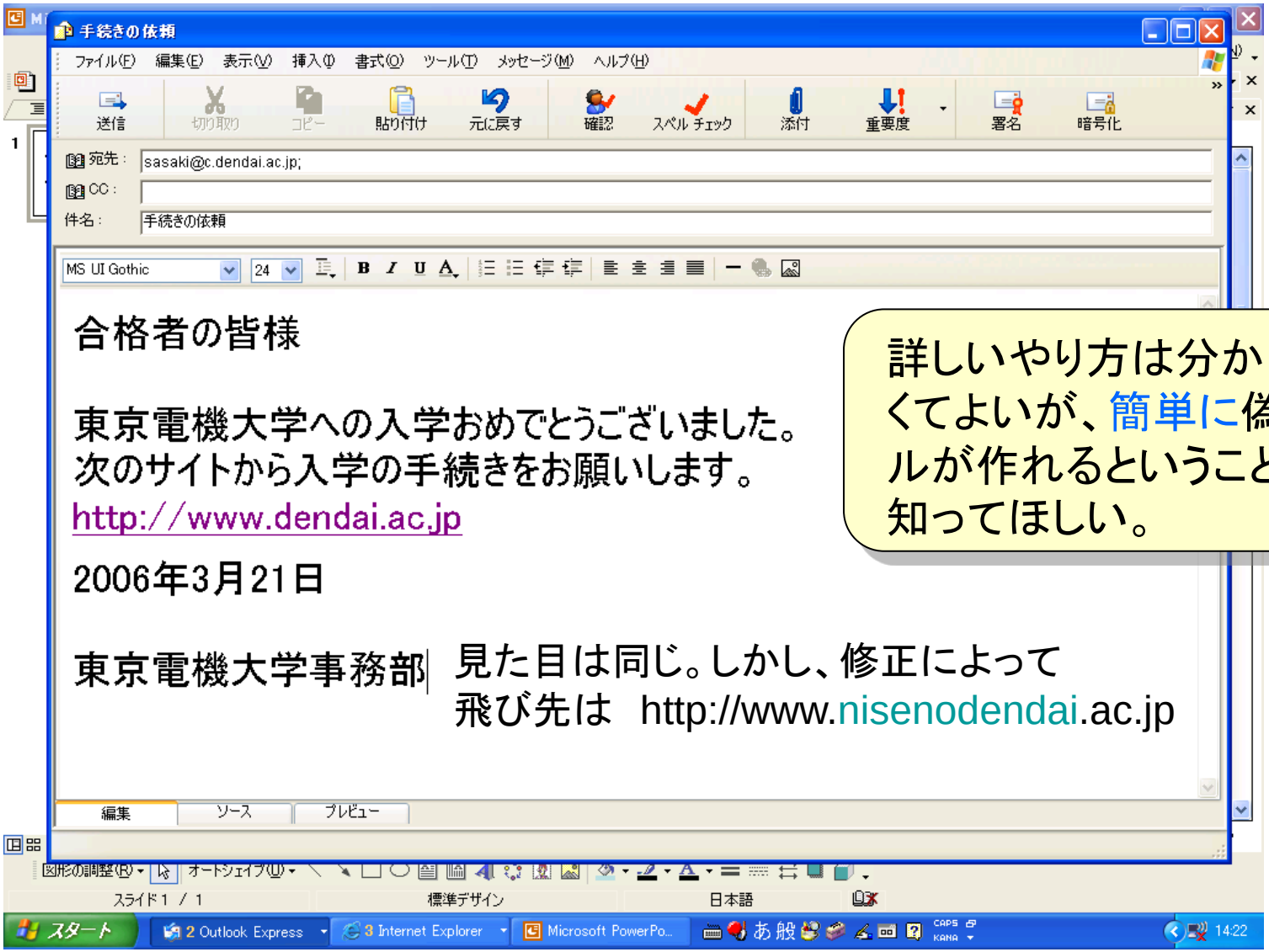
```
<DIV><FONT size=6><A
href="http://www.dendai.ac.jp">http://www.dendai.ac.jp</
A></FONT></DIV>
```

（5）ソースを変更し、表示と飛び先URLを異なったものにする。

（IPアドレスでもよい）

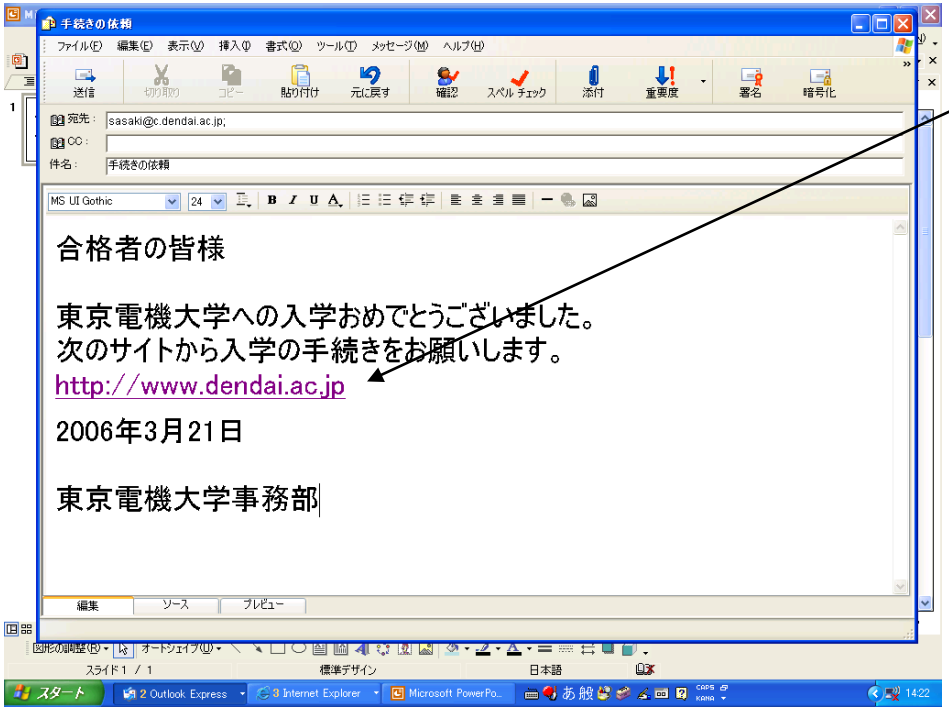
```
<DIV><FONT size=6><A
href="http://www.nisenodendai.ac.jp">http://www.dendai.a
c.jp</A></FONT></DIV>
```

Phishingメールの一例



フィッシングに対する主な対策（1）

1．メールに書かれているリンクを安易にクリックしない



メールの文中にあるリンクをクリックせず、ブラウザのアドレスバーに直接URLを入力する。

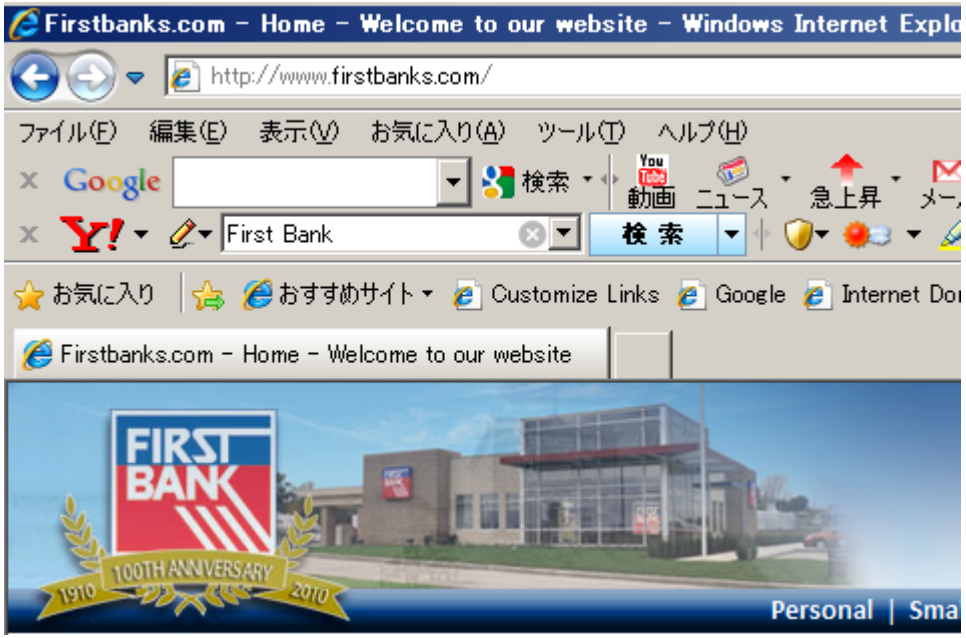
あるいは、URL部をコピーして、ブラウザーのURL部にペーストする。

これも絶対ではない。
（DNSポイゾニングなどの攻撃をされると不正サイトへ）

フィッシングに対する主な対策（2）

2．URLが怪しくないかどうかの確認

本物



絶対的な判断は難しい
（最近では正しいURLを上書きしたものも）

偽者

この例では、IPアドレスが直打ち（98.224.141.126）になっている

その他：HTTPSになっているものは、本物であることが多い

フィッシングに対する主な対策（3）

フィッシング対策機能を備えたセキュリティソフトを利用

2019年の保護率

カスペルスキー　94%
ウイルスバスター　97%

ウイズコロナ時代における詐欺メール

保健所をかたる詐欺メール

Von 京都府山城南保健所福祉室 <d2@ajasun.com> ☆
Betreff 通知 2020 Jan 29
An [redacted]

管内　通所・施設系障害福祉サービス事業者　様

お世話になっております。

新型コロナウィルス関連肺炎については、中国武感市を中心に患者が報告され、
国内でも岐阜県 で患者が報告されているところであり、

つきましては、別添通知をご確認いただき、
感染予防対策についてよろしくお願いいたします。

https://www.itmedia.co.jp/news/articles/2004/23/news027.html

© Can Stock Photo

マスクの提供

新型コロナウイルスによる肺炎が広がっている問題で、マスクを無料送付確認をお願いします
http://- [redacted]

https://www.jc3.or.jp/topics/newmodel_coronavirus.html

マンインザブラウザー攻撃

http://www.hitachi-systems.com/solution/s106/phishwall/mitb/

マン・イン・ザ・ブラウザ（Man in the Browser、MITB）とは、トロイの木馬などのマルウェアによってウェブブラウザの通信を監視し、オンラインバンキングへのログインを検知すると通信を乗っ取り、振込先を改ざんして預金を盗む攻撃である。中間者攻撃よりも容易で、かつ、防止が困難である。
＜2015年ごろから増加＞

攻撃者と攻撃方法の分類

1．部外者
（a）クラッカー
（b）スパイ
（c）テロリスト
（d）犯罪者等
2．部内者
（a） 従業員
（b）アルバイト等

直接的攻撃

コンピュータを直接的に操作し、不正アクセスを行いネットワーク上やファイル内のデータを攻撃

間接的攻撃

ソフトウエアをコンピュータに送り込む事によりファイルなどを攻撃
→ ウイルス

不正侵入方法の分類

不正行為

不正目的

内部に侵入しての攻撃

（1）パスワードの解明
（不正入手、類推攻撃他）

（2‘）セキュリティホールを利用した侵入
（sendmail
INN等）

（3）暗号化パスワードファイルの入手、解読

（4）他人への成りすましによる不正ログイン

（2）セキュリティホールを利用した直接的侵入
（バッファオーバフロー攻撃など）

外部からの攻撃

（5）Denial Of Service（DOS）攻撃
正当な利用者を使えなくする（Smurf攻撃等）

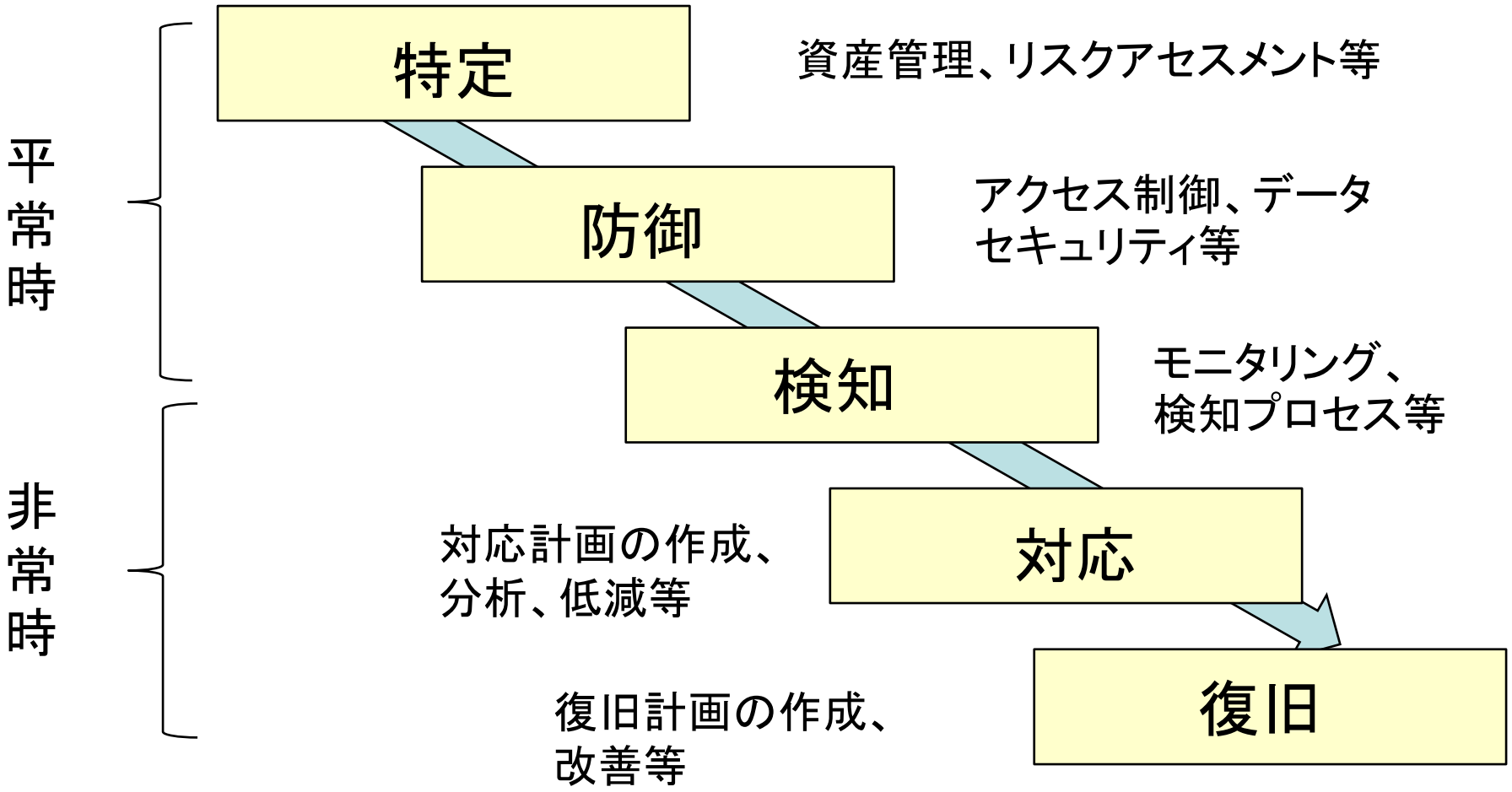
目的とする情報の取得

目的とする情報の改ざん

目的とする資源の利用

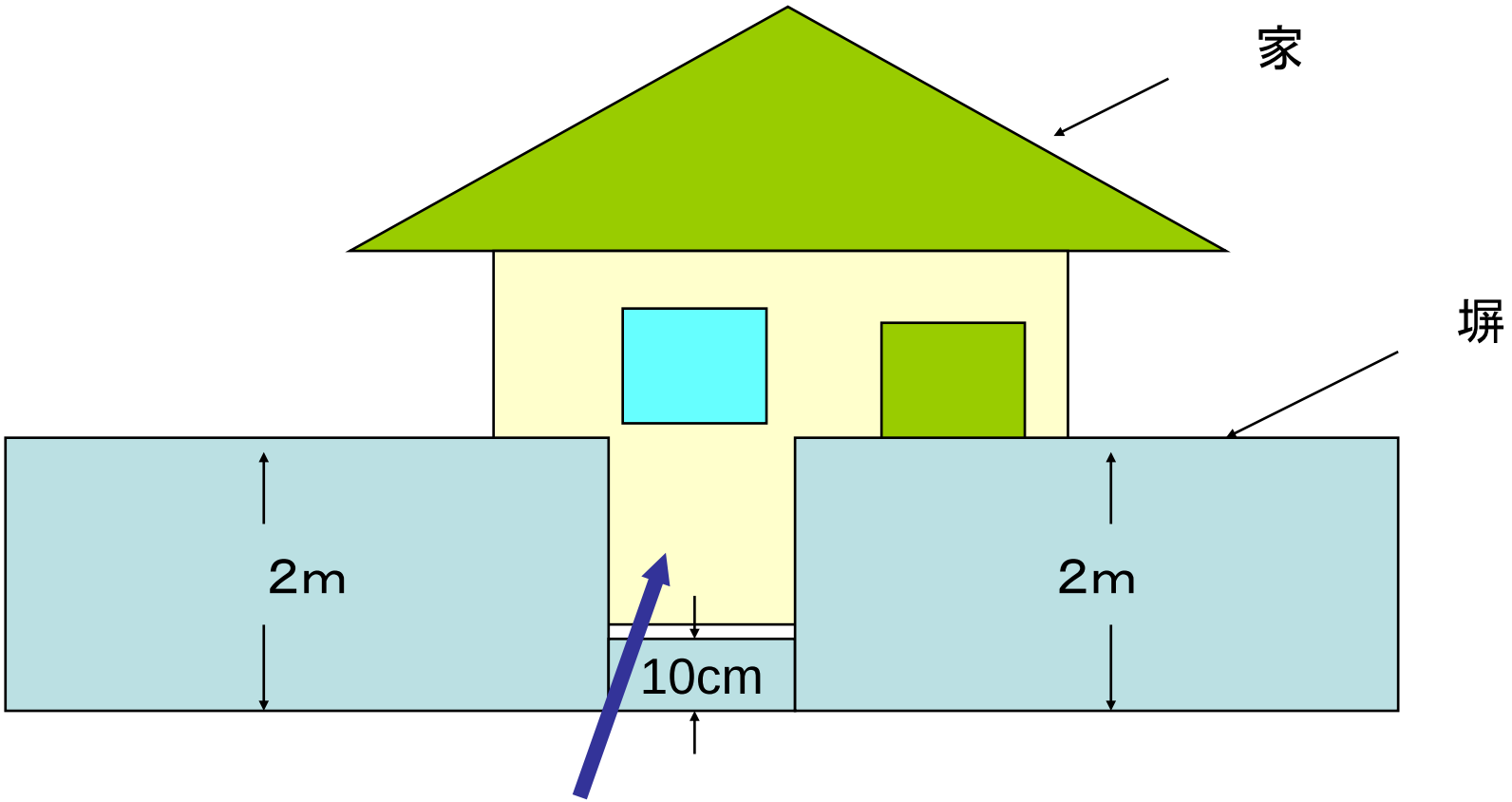
目的とする計算機の稼動停止

情報セキュリティの対策フェーズ



NISTの　Cyber Security　Frameworkによる分類

セキュリティ対策の効果のイメージ



リスクとは

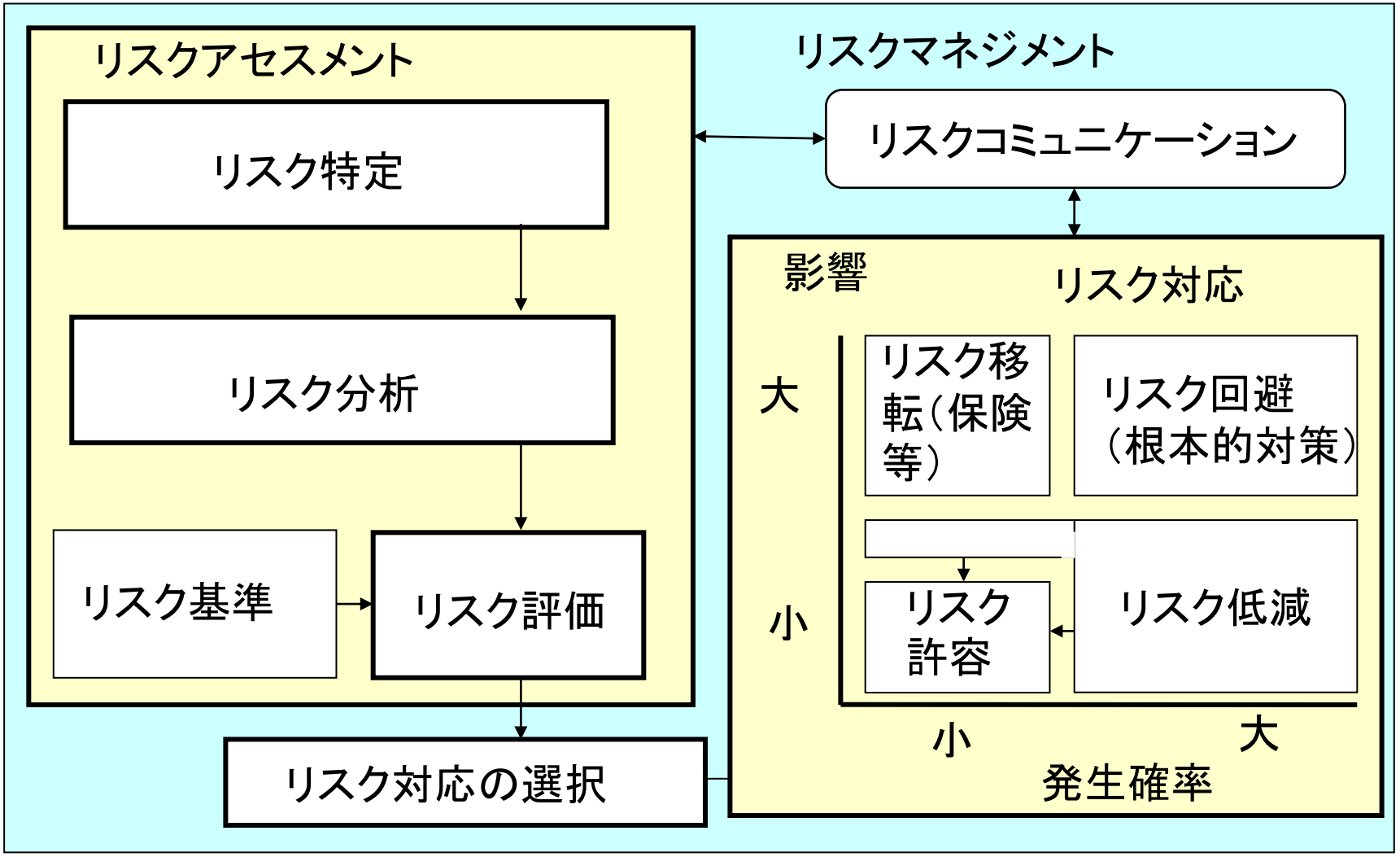
1．リスクとは，英語のRiskの訳であり，危険と訳される場合もある．「**将来の帰結に対する現在における予測**」という見方が下敷きになっていて常に**不確実性**を伴う。

2．工学分野の確率論的リスク評価では通常次のように定義することが多い。
　　リスク＝損害の大きさ　×損害の発生確率

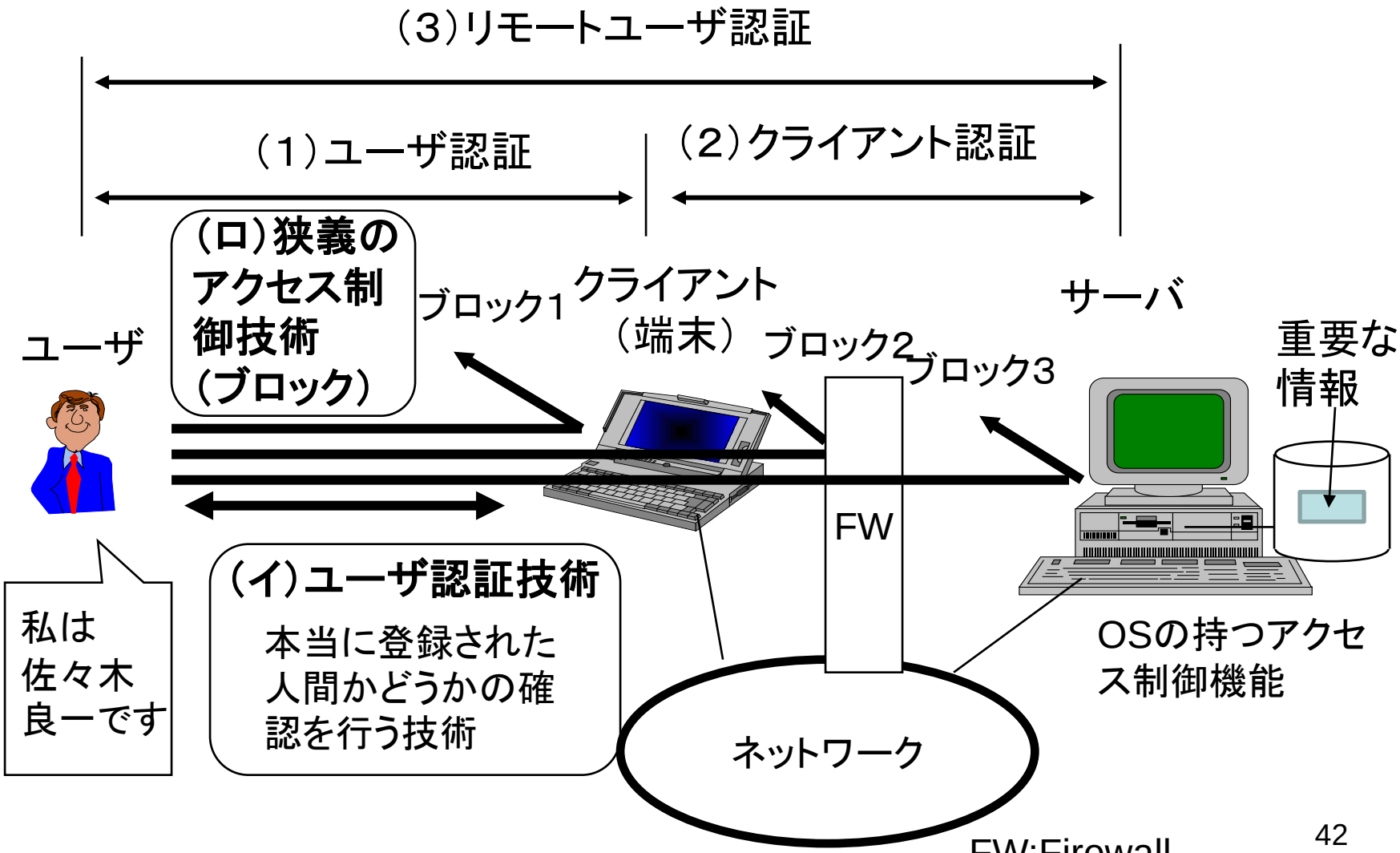
3．「ISO/IEC 27005：2008」ではITのリスクを以下のように定義しているが、結局同じことを表している。
　　リスク＝資産価値 × 脅威 × 脆弱性

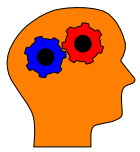
（注）英語のRiskが登場するのは1660年代。ハザードや災いを意味するイタリア語risicoからの転用

リスクマネジメントの要素と相互関連



アクセス制御技術の概要





ユーザ認証技術

本人確認（クライアント側）

- 本人の知識を利用するもの
  暗証番号、パスワード、パスフレーズ等
- 本人の持ち物を利用するもの
  磁気カード、ICカード（スマートカード）等
- 本人の身体的特徴を利用するもの
  指紋、声紋、虹彩等

リモートユーザ認証　　上記＋第3者による認証

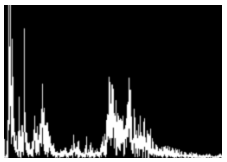
（1）クライアントの認証結果を利用するもの
（2）認証局を利用するもの（PKI）
（3）認証サーバを利用するもの（ケルベロス）

表　ユーザ認証方式の比較

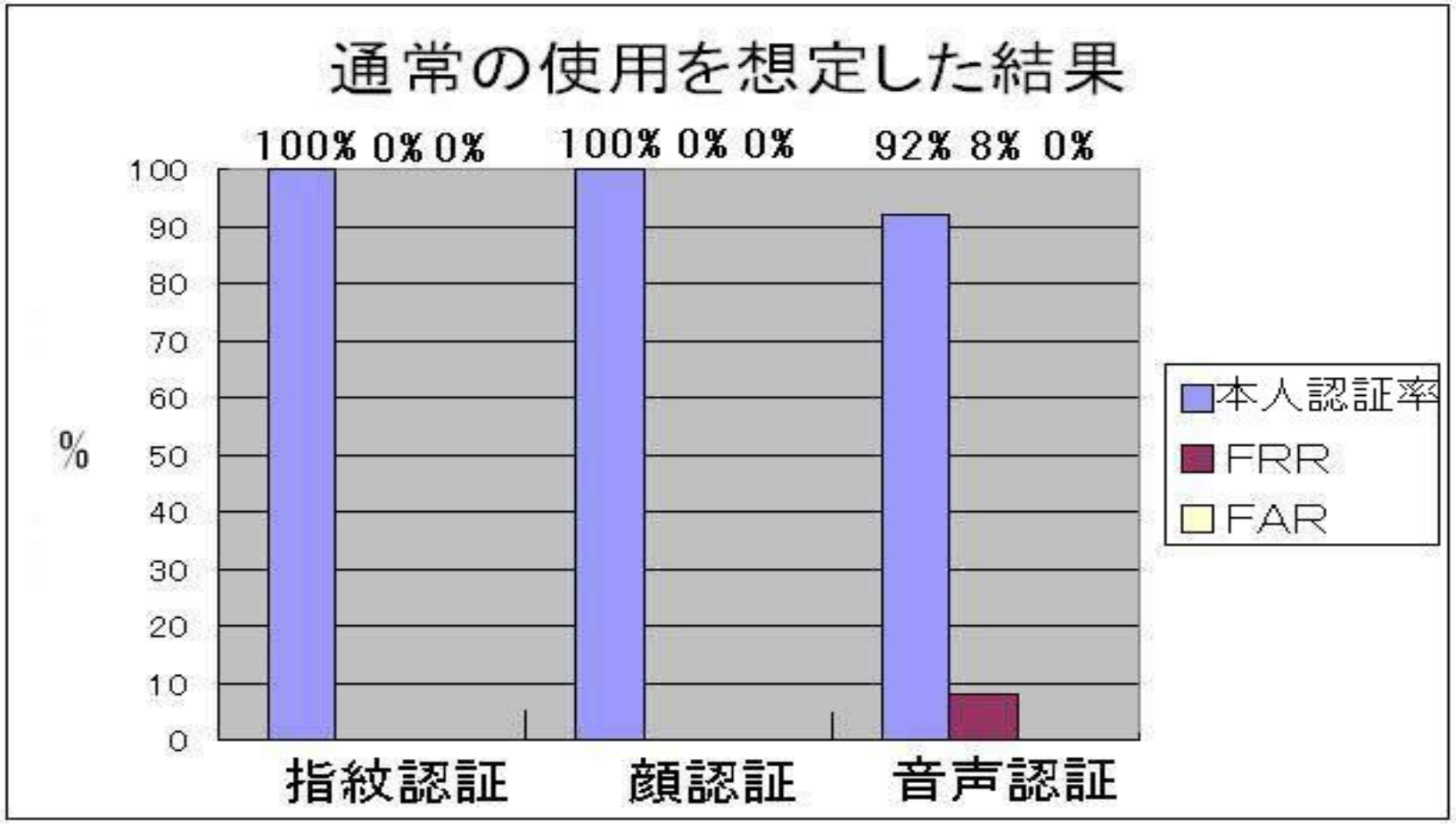
No	認証の根拠	例	長所	短所
1	知識	暗証番号 パスワード	実装が容易	忘れる危険性 類推が可能
2	持ち物	磁気カード ICカード	偽造が困難	なくする可能性 特別な読取装置が必要
3	身体的特徴（バイオメトリックス）	指紋 声紋 虹彩 網膜パターン	他人の偽造が困難 確実性が高い	プライバシー問題 変更が不可能 特別な装置が必要

携帯電話における生体認証の利用状況

NTT DOCOMOが扱っている携帯電話の種類：54 (Jan. 2009)	生体認証の利用機種：19
	生体認証を利用していない機種：35

認証方式	種類（%）
顔認証 	12 (22%)
指紋認証 	6 (11%)
音声認証 	1 (1.9%)

通常の認証方法を想定した実験結果



※FRR(本人拒否率)　FAR(他人許容率)

人工指作製手順

※松本研究室“人工指の研究”週刊バイオ第33号

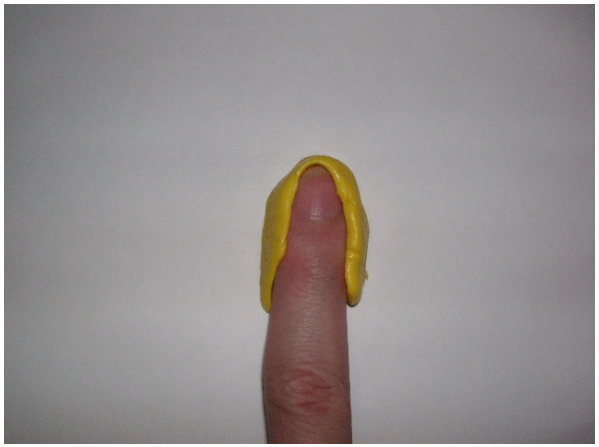
A) プラステック樹脂を60℃以上の湯に浸し、柔らかくなったら生体指を押し当て型を取る

B) 型が硬化したら（約10分間）生体指を取り外す

C) 湯：ゼラチンを1:1の割合でゼラチンを溶かす

D) A,Bで作製した型に溶けたゼラチンを流し込む

E) 冷蔵庫に入れ、ゼラチンが硬化したら完成



人工指を用いた実験手順

- 人工指作製手順に従い、登録者の人工指を作製する
- 登録者自身の指と、登録者の人工指を用いて認証を試みる

写真と画像を用いた認証実験手順

A) 登録者の顔写真を用意する

B) 登録者の顔を写した画像を用意する

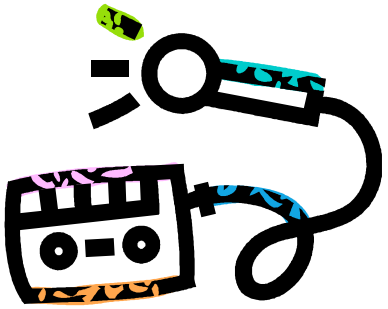
C) 顔認証の登録と認証を、本人の顔、顔写真、
顔画像を用いて全てのパターンで認証を試みる

録音機器を用いた実験手順

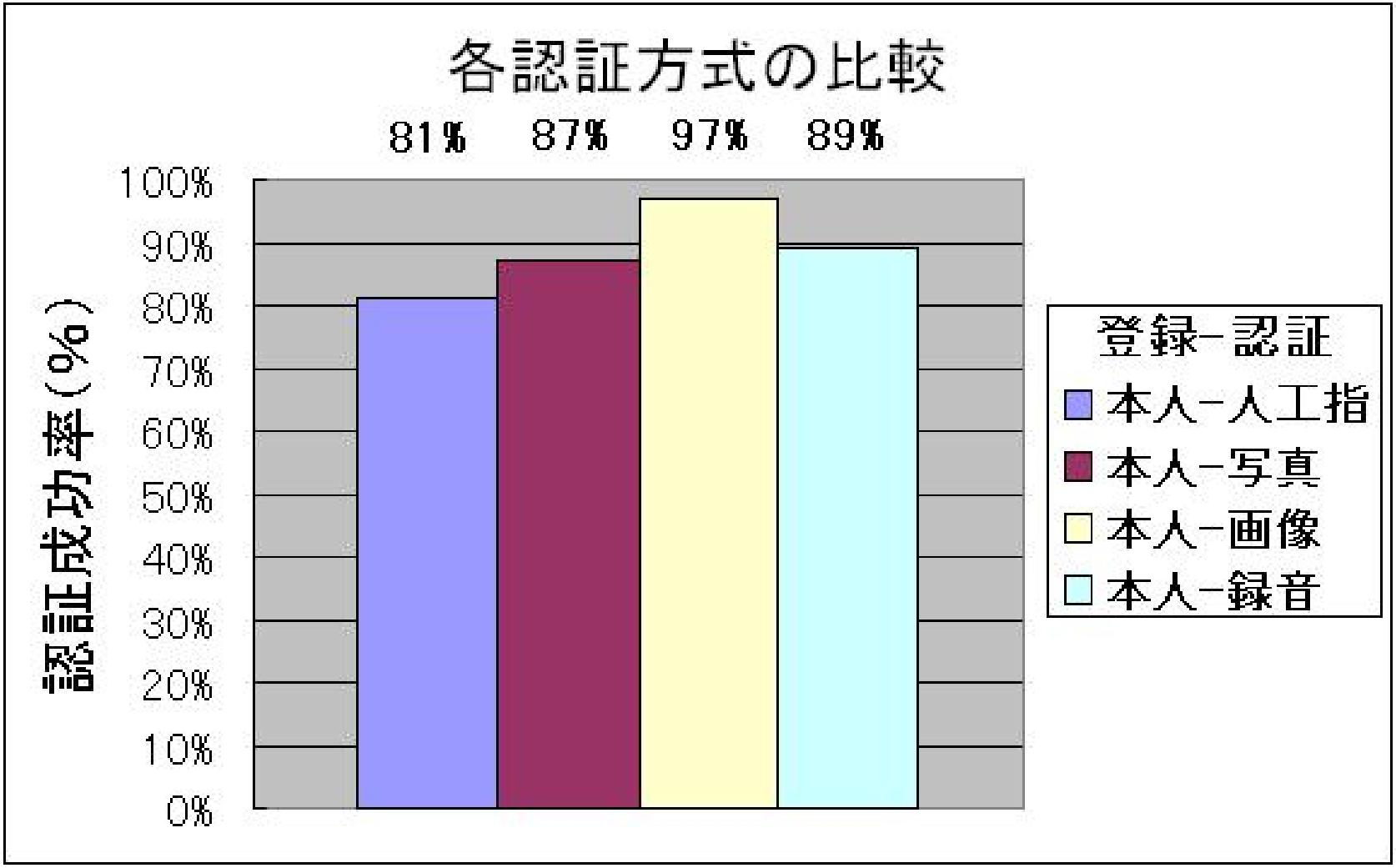
A) 録音機器にマイクを接続して、「デンキダイガク」と発音する

B) 録音した音声をPCに取り込み、再生する

C) スピーカーから出力された音声を携帯電話で認証



各認証機器の認証成功率の比較

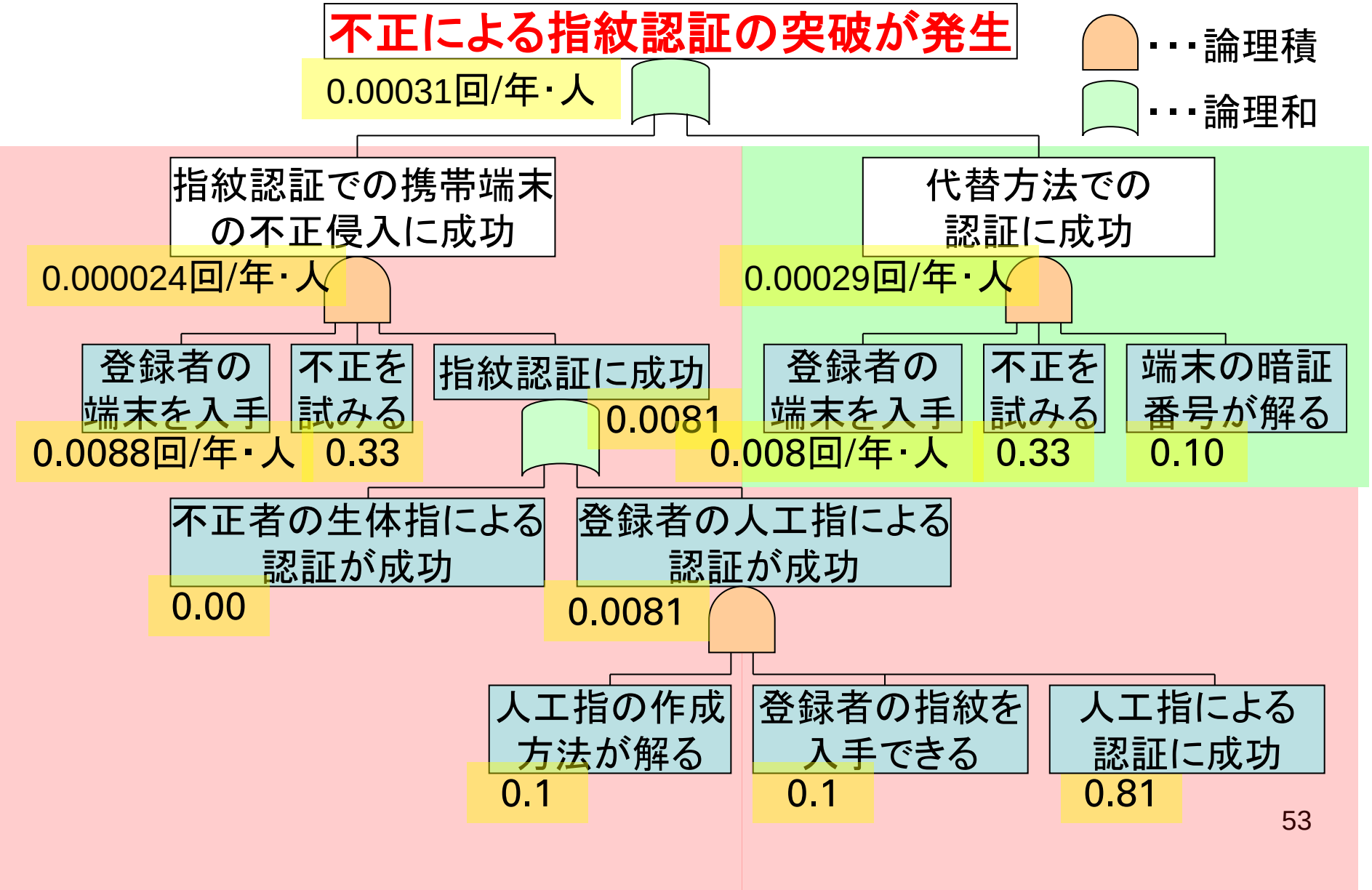


FTA（フォルトツリー分析）

1. 初めに望ましくない事象を定義する
2. その事象を発生させる要因を摘出する
3. システムの故障を発生させる事象との因果関係を、論理記号を使用してツリー状に表現する
4. 各事象ごとの故障率を割り当てる

サイバー攻撃の分析に用いる場合はアタックツリー分析ともいう

FTA（指紋認証）


不正による指紋認証の突破が発生
0.00031回/年・人
・・・論理積
・・・論理和
指紋認証での携帯端末の不正侵入に成功
0.000024回/年・人
代替方法での認証に成功
0.00029回/年・人
登録者の端末を入手
0.0088回/年・人
不正を試みる
0.33
指紋認証に成功
0.0081
登録者の端末を入手
0.008回/年・人
不正を試みる
0.33
端末の暗証番号が解る
0.10
不正者の生体指による認証が成功
0.00
登録者の人工指による認証が成功
0.0081
人工指の作成方法が解る
0.1
登録者の指紋を入手できる
0.1
人工指による認証に成功
0.81

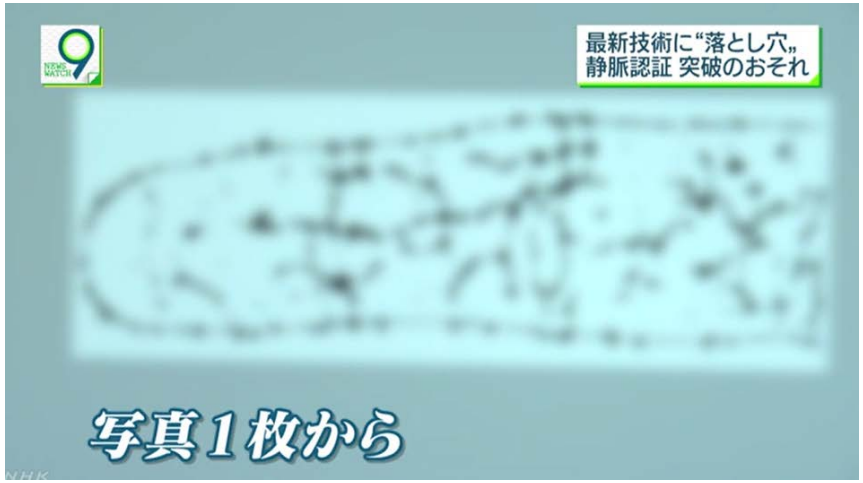
考察

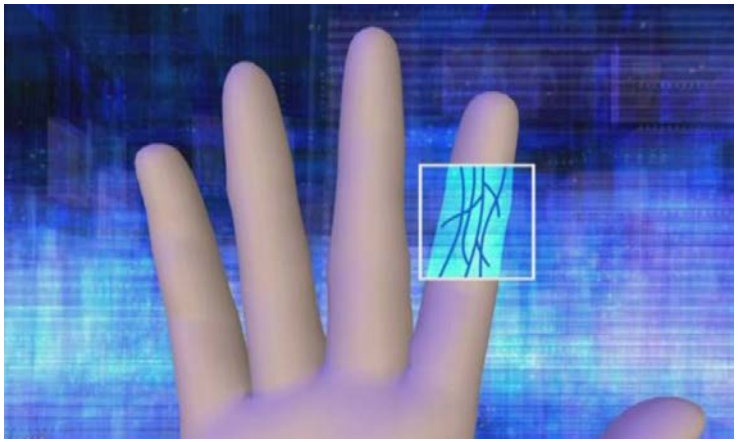
(1)これをどういうように考えるべきか？
　(a)個人としてはほとんど心配する必要がない
　(b)1億人が使っているので社会全体としてはさらに対策の検討が必要

(2)2020年時点ではどうか？
　(a)現在でも同様なリスクは存在。さらに4Kテレビ、8Kテレビなどが出ると、画像から人工指の指紋作成が容易
　(b)静脈認証を使っていると従来のものよりは安全性は高い。しかし過信は禁物

指の静脈の生体認証
デジカメ画像で突破される危険

国立情報学研究所の越前功教授らの研究グループは、市販のデジタルカメラで研究員２人の指を50センチの距離から１本ずつ撮影したうえで、指の画像を特殊な方法で加工すると、静脈が浮かび上がり、そのパターンを読み取れることを確認しました。





https://www3.nhk.or.jp/news/html/20181101/k10011694811000.html

最近は2要素認証・2経路認証など

目次

サイバー攻撃の歴史

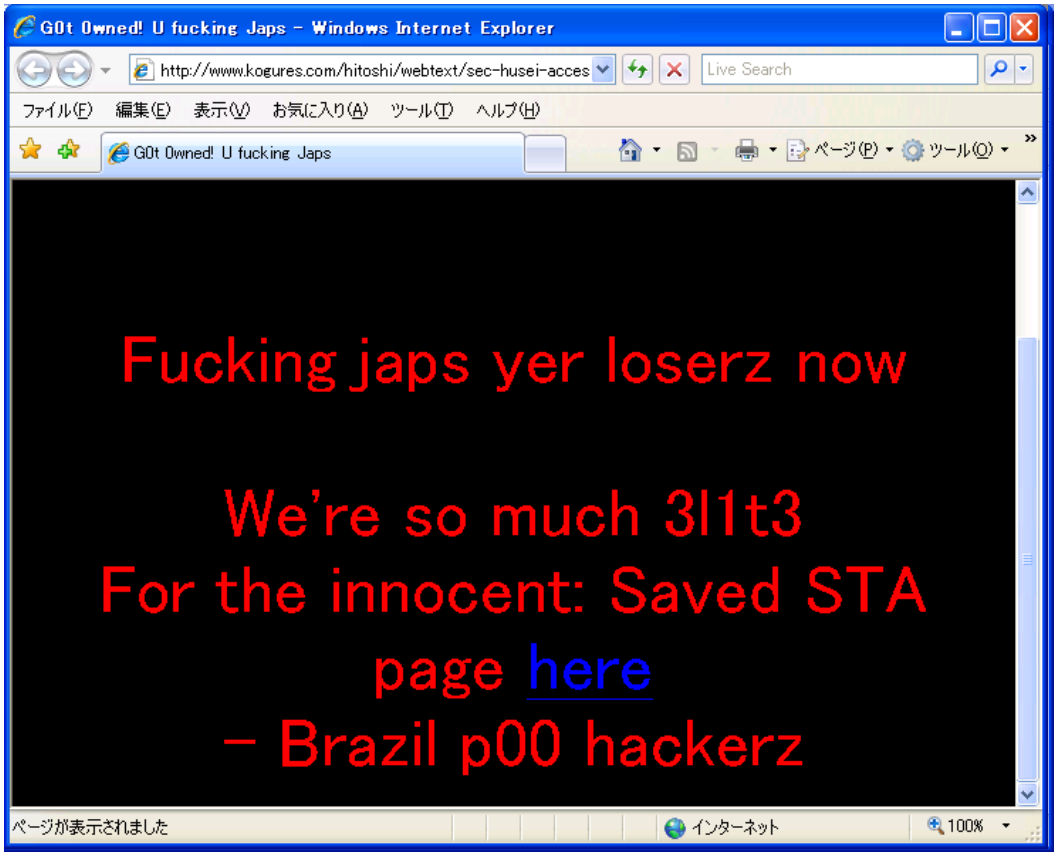
＜セキュリティにとっての第一のターニングポイント＞

2000年　科学技術庁などのホームページの改ざん事件
2000年　　不正アクセス禁止法施行
2000年　　JNSA発足（2001年NPO化）
2001年　Code　Red、Sircumによる被害
2001年　　電子署名法施行
2001年　　CRYPTREC（暗号技術検討会）発足

＜セキュリティにとっての第二のターニングポイント＞

2010年　Stuxnetの出現(遠心分離機への攻撃)
2011年　　ウイルス作成罪施行
2011年　三菱重工などへの標的型メール攻撃
2015年　日本年金機構への攻撃

科学技術庁ホームページ改ざん事件



2000年1月

Reference：http://www.kogures.com/hitoshi/webtext/sec-husei-access/homepage.html

サイバー攻撃の歴史

＜セキュリティにとっての第一のターニングポイント＞

2000年　科学技術庁などのホームページの改ざん事件
2000年　　不正アクセス禁止法施行
2000年　　JNSA発足（2001年NPO化）
2001年　Code　Red、Sircumによる被害
2001年　　電子署名法施行
2001年　　CRYPTREC（暗号技術検討会）発足

＜セキュリティにとっての第二のターニングポイント＞

2010年　Stuxnetの出現(遠心分離機への攻撃)
2011年　　ウイルス作成罪施行
2011年　三菱重工などへの標的型メール攻撃
2015年　日本年金機構への攻撃

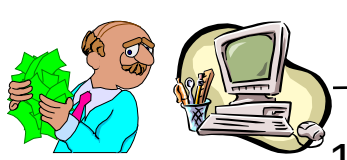
2つのターニングポイントの比較

	第一次ターニングポイント（2000年ごろ）	第二次ターニングポイント（2010年以降）
攻撃目的	面白半分	多様化（面白半分、主義主張、お金儲け、国家の指示）
攻撃者	ハッカー（クラッカー）	ハッカー、ハクティビスト、犯罪者、スパイ、軍人
攻撃対象	WEBなどの一般IT	重要情報インフラも＜Stuxnet＞
攻撃パターン	不特定多数	標的型＜Stuxnet、ソニー、三菱重工、日本年金機構＞
攻撃技術	低ー中	中ー高　＜Stuxnet、ソニー、三菱重工、農林水産省 ＞

従来の攻撃が風邪なら、新しい攻撃は新型インフルエンザ

日本年金機構への標的型攻撃

①標的型メール送信
（ウイルス付き）
2015年5月18日から22日



124通

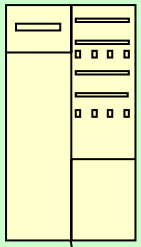
攻撃者

日本年金機構

4名

② 添付ファイルを開封など＝＞感染（ワクチンチェックをしても検知不能）

基幹システム（社会保険オンラインシステム）



③C&Cサーバとのやり取り

C&Cサーバ

④感染の拡大（約31台）

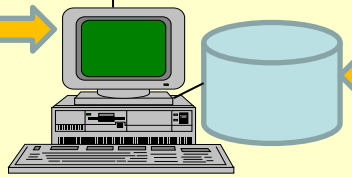
感染PC

抽出

港区海運業者サーバ（踏み台）

感染PC（データ保管）

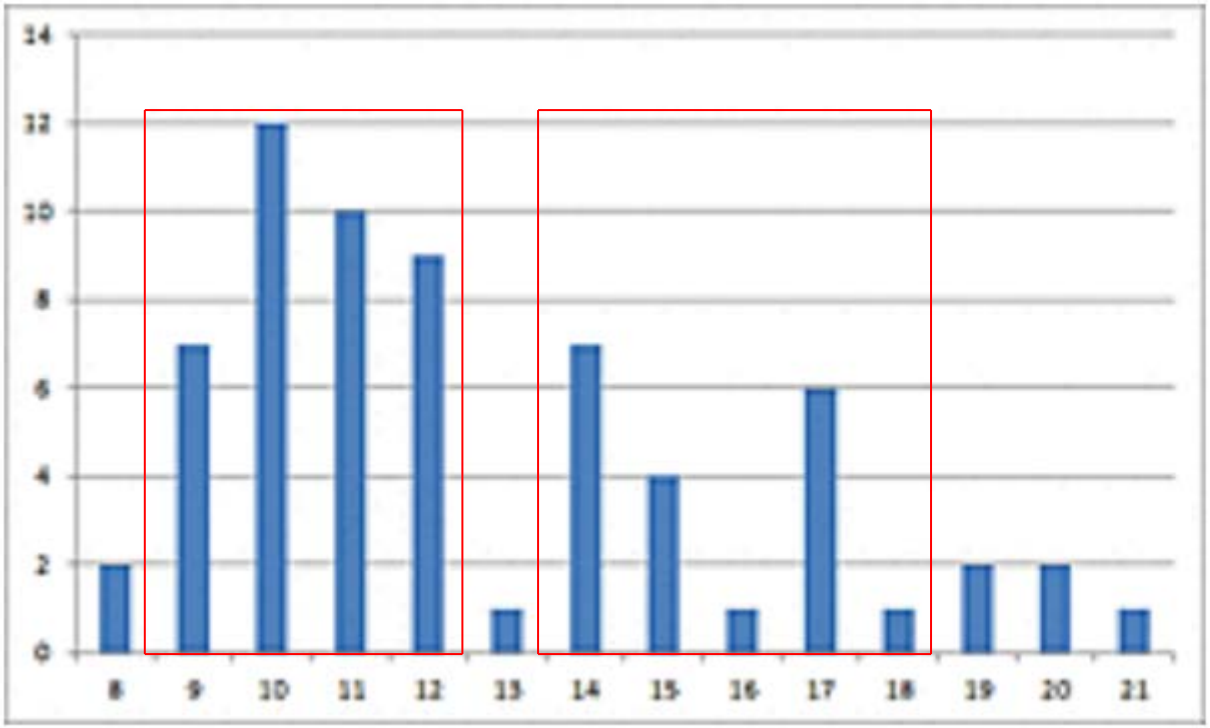
アクセス



年金加入者個人情報（約125万件：対象者は約101万人）

⑤ 個人情報の流出

ウイルスが作成された時刻分布



標準時間
＋8時間

10:00AM付近を中心に午前中に作成された検体が多いようですが、全体的に、だいたい一般的な民間企業や公的機関の労働時間に収まっているようです。

http://blog.macnica.net/.s/blog/2015/06/emdivi-201405-eea5.html

米国政府での情報漏えい

米連邦政府の人事管理局（OPM）がサイバー攻撃を受けて職員らの個人情報が大量に盗まれた事件で、OPMは2015年7月9日、新たに政府機関の職員や契約業者ら計2150万人分の身元調査に関わる情報が盗まれていたと発表した。
OPMは6月に約420万人分が盗まれたと発表している。米紙ワシントン・ポスト（電子版）によると、流出した情報には重複があり、2件のサイバー攻撃で合計2210万人分になるという。同紙は、米国政府史上で最も深刻なサイバー攻撃被害だと指摘した。

被害は日本だけではない

http://mainichi.jp/select/news/20150710k0000e030169000c.html

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化
   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化
   PCなどからIoTなどへ
4. 攻撃者の多様化・高度化
   犯罪組織の高度化
   国家を後ろ盾とした攻撃の増加

仮想通貨580億円相当不正流出

国内仮想通貨取引所を運営する「コインチェック」は26日、同社の取引所から約580億円相当の仮想通貨が不正に流出したと発表した。

同社は、取り扱うすべての仮想通貨の出金を一時停止した。外部から不正アクセスの形跡があり、サイバー攻撃の可能性がある。金融庁と警視庁に報告した。

不正流出したのは、仮想通貨の「ネム」で、同取引所が預かっていた全額が流出した。

2018年1月27日

https://mainichi.jp/articles/20180127/k00/00m/040/260000c

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化

   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化

   PCなどからIoTなどへ
4. 攻撃者の多様化・高度化

   犯罪組織の高度化

   国家を後ろ盾とした攻撃の増加

ランサムウエア

ランサムウェア（Ransomware）とはマルウェアの一種である。
これに感染したコンピュータはシステムへのアクセスを制限される。この制限を解除するため、マルウェアの作者へ身代金の支払いが要求される。
数種類の形態のランサムウェアは、システムのハードディスクドライブを暗号化し（**暗号化ウイルス恐喝**）、また他の幾種類かは単純にシステムを使用不能にし、ユーザーに対して身代金を支払うようにそそのかすメッセージを表示する。

＜データの暗号化という意味では完全性の喪失
データを使えないという意味では可用性の喪失＞

ランサムウェアの被害を防ぐために必須の対策

（1） こまめにバックアップする

（2） OSやソフトの脆弱性を修正する

（3） メールのリンクや添付ファイルを安易に開かない

（4） セキュリティソフトを最新の状態で利用する

https://www.is702.jp/special/2160/ 2017/06/22 トレンドマイクロ

ランサムウエアへの対応法

1．バックアップやクラウドストレージから戻す方法（正規の方法）

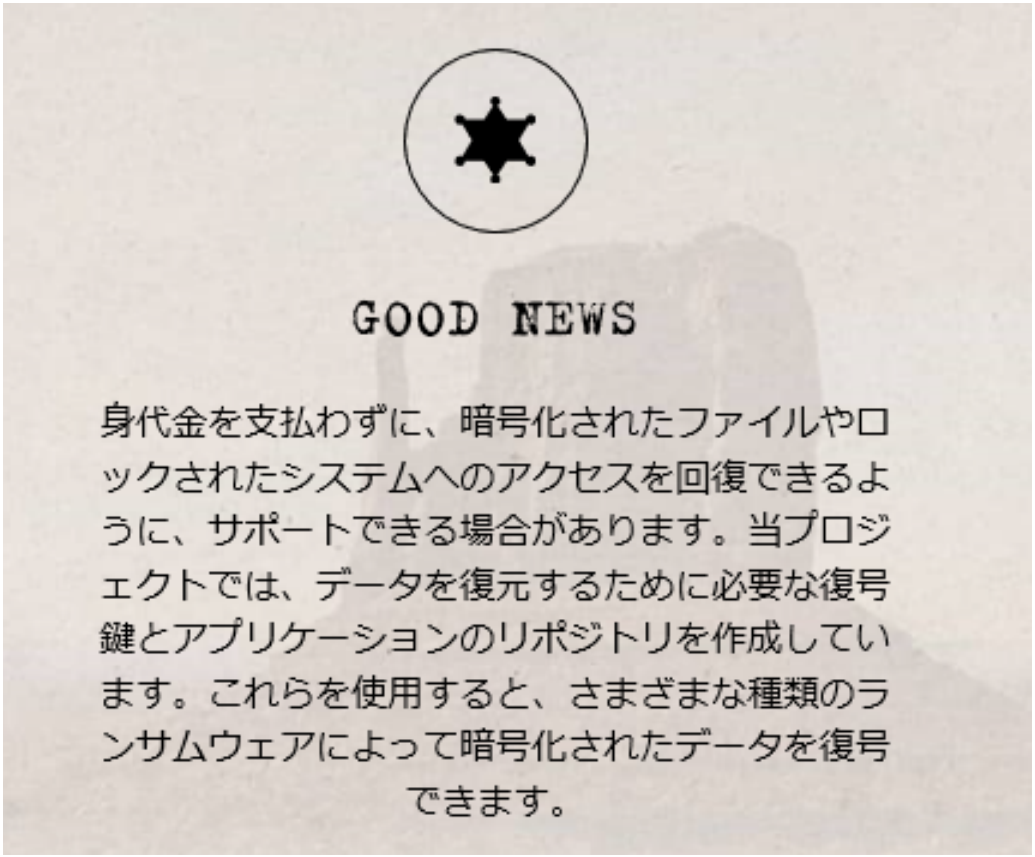
2．ボリュームシャドウコピーで復元させる方法（これも可能）

3．削除ファイルの復元ツールを使う方法

平文を暗号化した後、平文フアイルを単純消去するだけなら復元ツールで復元可能（単純消去だけの可能性は低い）

4．メモリー上のデータのダンプをとることによる暗号かぎの取り出し（可能性は低い）

No More Ransom Project



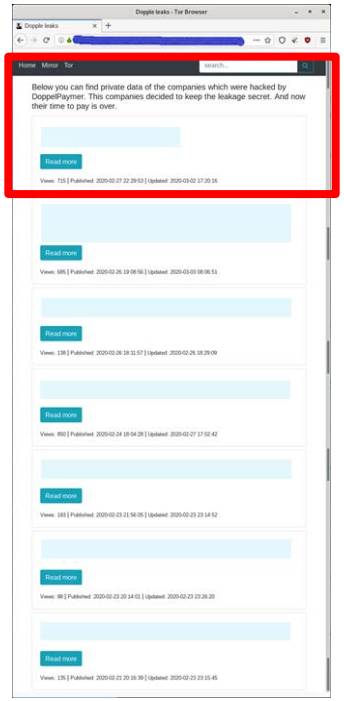
各ランサムウエアを調査し、メモリー上のデータのダンプをとることなどにより復号かぎの取り出しを行ったと考えている

EKANSは、復元化可能なランサムウエアのリストに入っていない

https://www.nomoreransom.org/ja/index.html

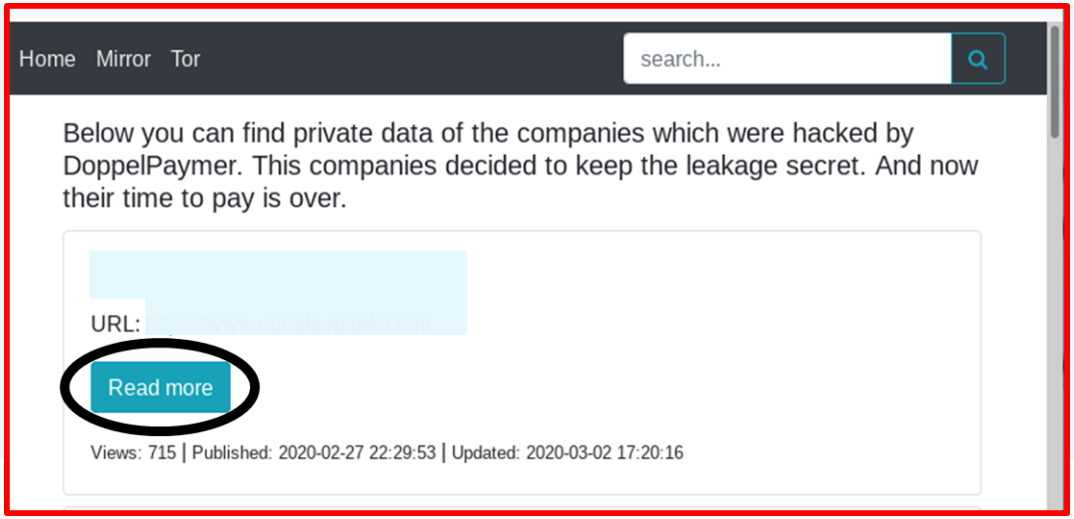
最近のランサムウエア　Dopple Leaks（暴露型ランサムウエア）

Doppelpaymer Ransomwareの身代金を支払わなかった被害者の情報を公開するために立ち上げた専用WEBサイト（現在β版）



Dopple Leaks“サイト
(3/6現在)

DoppelPaymer Ransomwareで盗み出した情報を公開することで、身代金支払いを促す効果がある
3月8日までに9社の一部データが公開されている



類似のものに「Maze」がある。

Mazeによる脅迫文

1．攻撃の3日後にWebで情報が公開される。3日以内にコミュニケーションができなかった場合、信用損失の責任は全て被害者側にある。

2．交渉とは、対話し、双方にとって最良の解決策を見つけることである。被害者側がシャイ、または恐れていることで交渉ができない場合、それは被害者側の問題だ。我々はそれを理解する学者ではない。

3．私たちの協力なしにデータを復元しようとする場合、1000万ドル規模の費用がかかることを理解する。

4．クライアントが交渉に失敗した場合、情報の公開が開始され、10日後には全ての情報が公開される。

5．公開開始後、被害者のパートナー、顧客、規制当局などに通報する。

身代金を払わない理由

1. 「身代金」を払ってもサイバー犯罪者が約束を守る保証はどこにもない

2. 身代金の支払いはサイバー犯罪者にさらなる攻撃のための資金を与えることになる

3. 身代金を支払ったことが理由で、別の犯罪や脅迫に巻き込まれる危険性もある

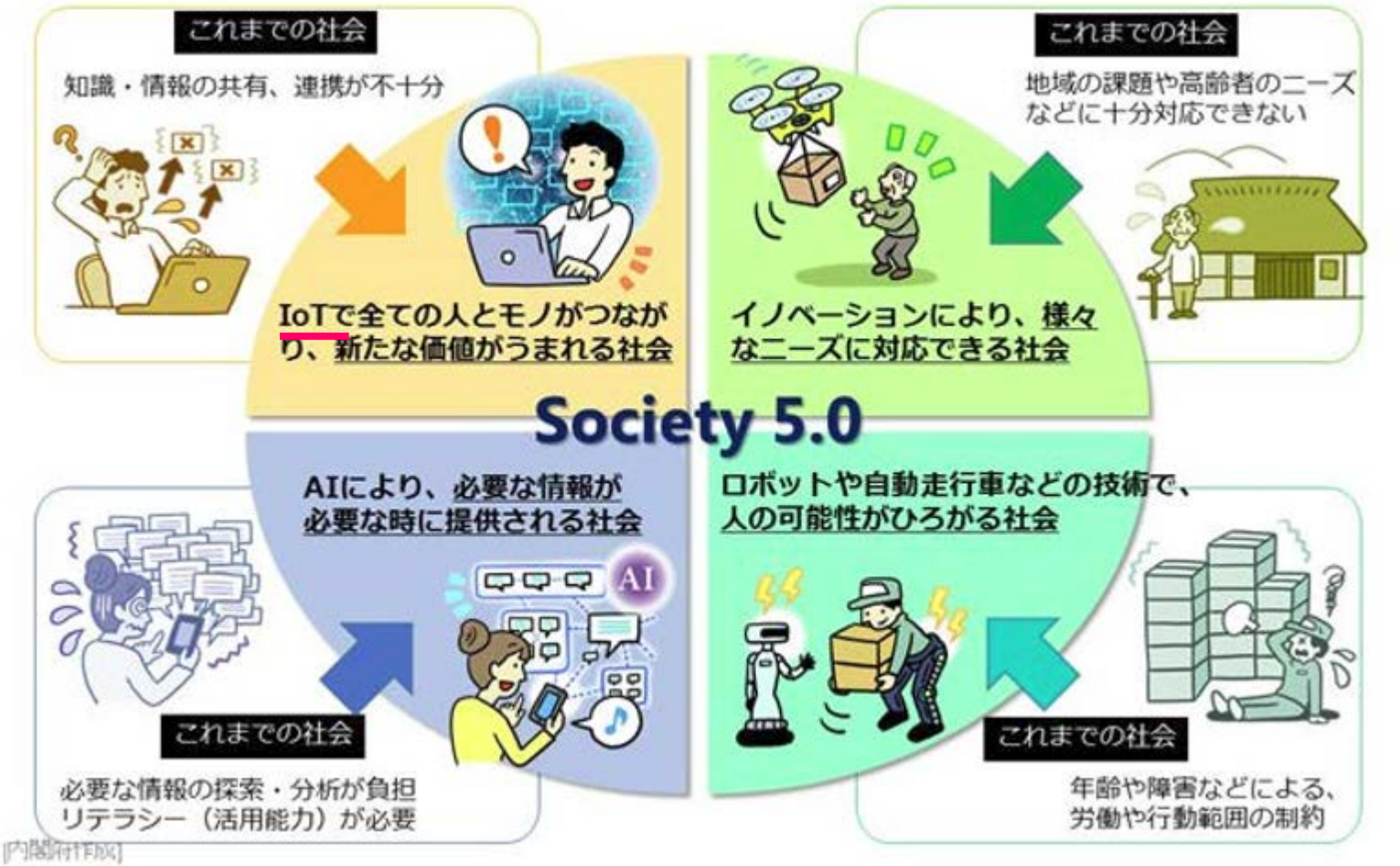
http://www.trendmicro.co.jp/cloud-content/jp/pdfs/doc-dl/ransomware-20160411-01.pdf

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化
   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化
   PCなどからIoTなどへ
4. 攻撃者の多様化・高度化
   犯罪組織の高度化
   国家を後ろ盾とした攻撃の増加

Society5.0で実現する社会

内閣府**第5期科学技術基本計画で提唱**



サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会

https://www8.cao.go.jp/cstp/society5_0/index.html

IoTの特徴とセキュリティへの影響

（性質１）脅威の影響範囲・影響度合いが大きい

（性質２）IoT 機器のライフサイクルが長い

（性質３）IoT 機器に対する監視が行き届きにくい

（性質４）IoT 機器側とネットワーク側の環境や特性の相互理解が不十分

（性質５）IoT 機器の機能・性能が限られている

（性質６）開発者が想定していなかった接続が行われる可能性がある

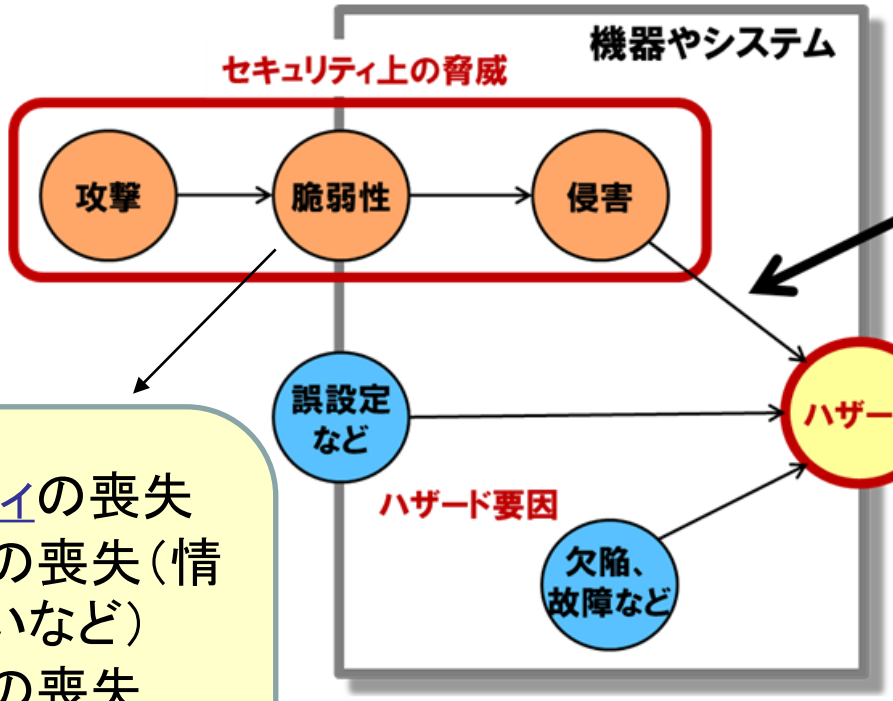
発生確率が大きい
影響が大きい
→ リスクが大きい

適切なセキュリティ対策がより重要に

セキュリティ対策が困難

左側はIoTセキュリティガイドライン　平成28年7月
http://www.soumu.go.jp/main_content/000428393.pdf　より

セキュリティとセーフティ

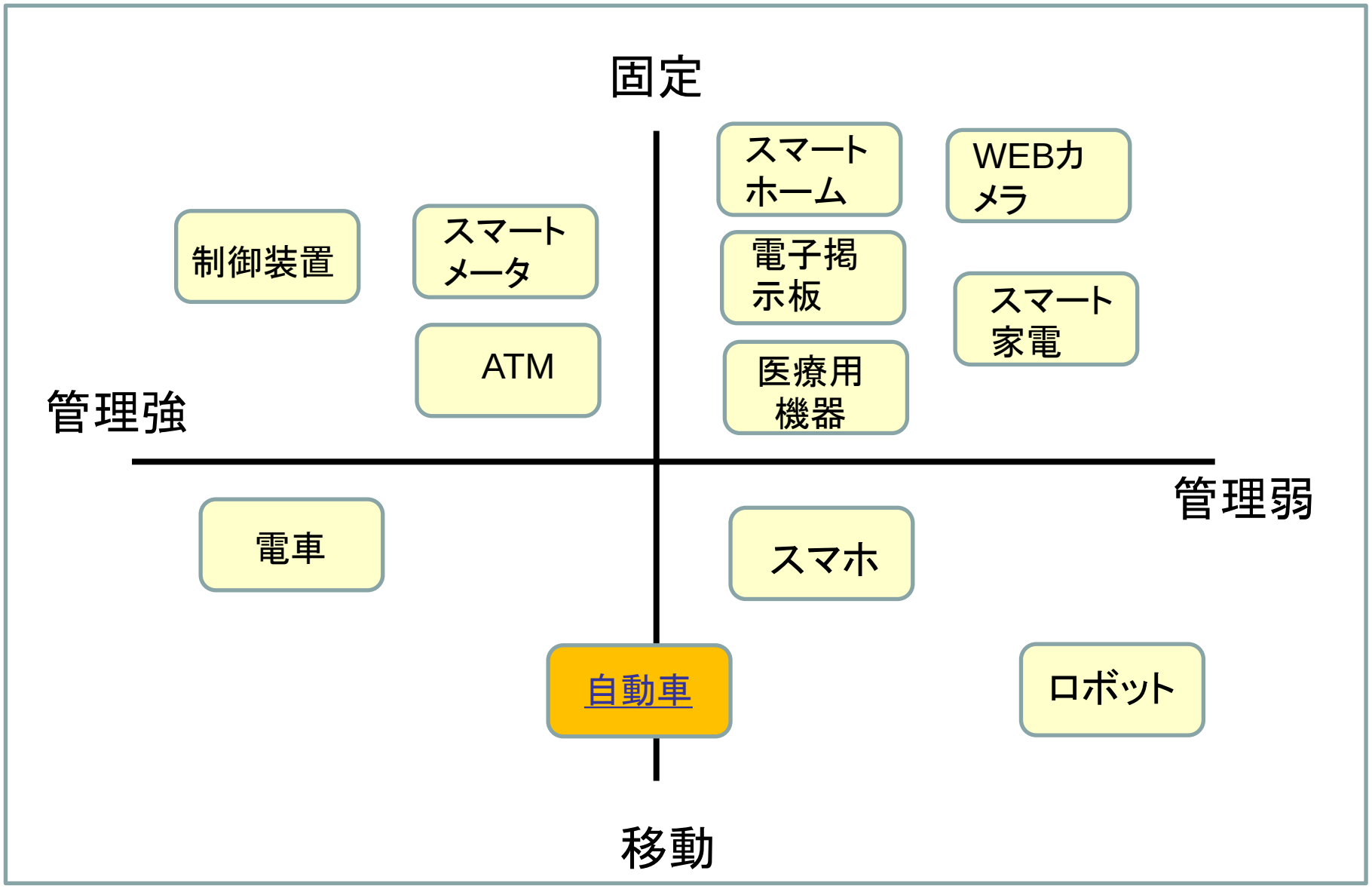


セーフティの喪失
環境影響
健康影響
業務停止
など

セキュリティの喪失
①機密性の喪失（情報の漏えいなど）
②完全性の喪失（データの改ざんなど）
③可用性の喪失（システムダウンなど）

IoTセキュリティガイドライン　平成28年7月
http://www.soumu.go.jp/main_content/000428393.pdf
をベースに追加

主要なIoT機器


固定
スマート
ホーム
WEBカ
メラ
制御装置
スマート
メータ
電子掲
示板
スマート
家電
ATM
医療用
機器
管理強
管理弱
電車
スマホ
自動車
ロボット
移動

自動車への具体的攻撃例

- Blackhat2015でCharlie Miller氏とChris Valasek氏がジープのチェロスキーの遠隔操作法を発表

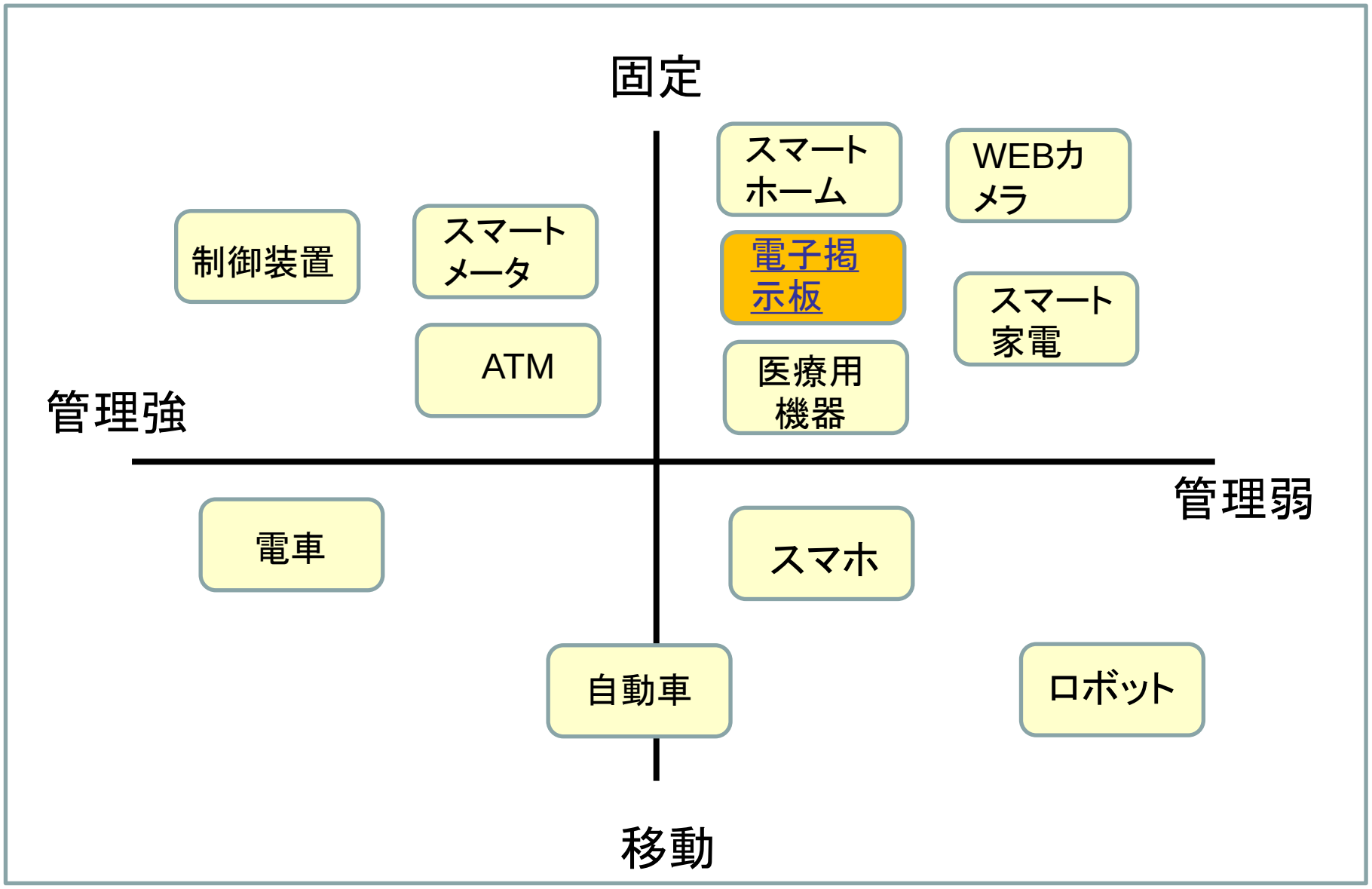
攻撃者は数マイル離れた自宅から

ハンドル操作
ブレーキの無効化
高速走行中のエンジンの停止など

140万台のリコールに

https://blog.kaspersky.co.jp/blackhat-jeep-cherokee-hack-explained/8480/

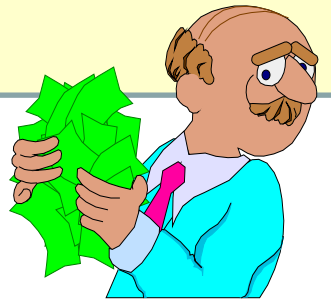
主要なIoT機器


固定
スマート
ホーム
WEBカ
メラ
制御装置
スマート
メータ
電子掲
示板
スマート
家電
ATM
医療用
機器
管理強
管理弱
電車
スマホ
自動車
ロボット
移動

交通標識が「ゴジラ来襲」と警告

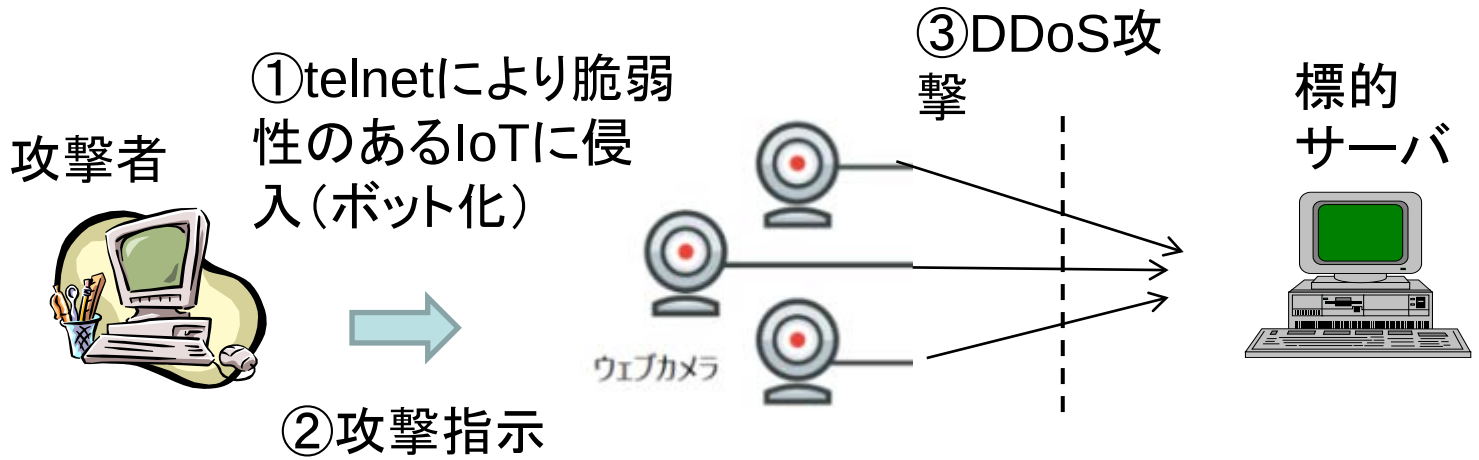
その他のIoTのセキュリティ

- WEBカメラ、家庭用ルータなどのIoTが攻撃の踏み台に
- 今後は家庭用ロボットなどのハッキングによる被害なども発生か



IoTを利用したDDoS攻撃

＜MiraiによるDDoS攻撃：2017年＞



620Gbps程度

DDoS（Dissributed Denial Of Service）攻撃（サービス不能攻撃ともいう）

サプライチェーンにおける脅威

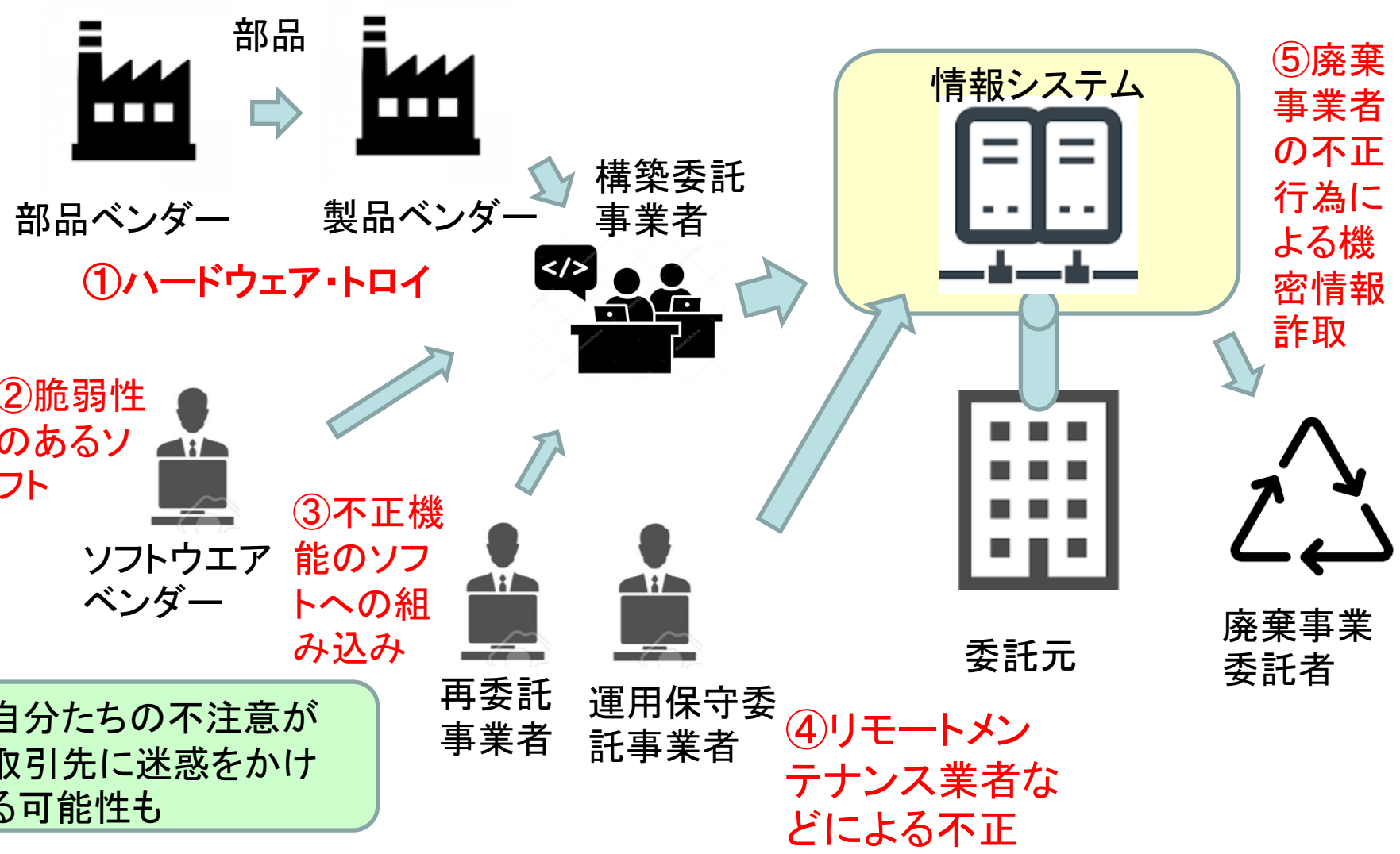
- 海外から調達した通信機器（中国の大手通信機器メーカー「ファーウェイHUAWEI」のルーター）がアメリカで深夜に勝手に動き本国にデータ送信の疑惑

- 中国のスマートフォンメーカーCoolpadが製造する多数のハイエンド向けAndroid端末にバックドア設置が発覚

  https://www.ipa.go.jp/files/000044089.pdf

⇨ NEDOでサプライチェーン対策システムの研究「IoT社会に対応したサイバー・フィジカル・セキュリティ」を開始

サプライチェーンリスクの図式化



https://blogs.mcafee.jp/scrm-risk-preventionを参考に作成

サプライチェーン対策の分類

（1） 発注先の限定

米国政府の中国大手通信機器メーカー「華為技術」および「中興通訊（ZTE）」の製品の排除　など

（2） 発注先に調達基準の設定と評価の実施

NIST SP800-171 rev.1 （連邦政府外のシステムと組織における管理された非格付け情報の保護）の制定

それに基づく企業グループでの活動　など

（3） 信頼のおけるサプライチェーン支援システムの導入

NEDOにおけるIoT向けサプライチェーン支援システムなど

残された課題

（1） 国家間の対立がある中で、一番の課題である信頼の創出部分の不正を防ぎきる仕組みを作れるか

（2） 高コストになりがち。

誰がコストを負担するのか。

エコシステムは存在するのか

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化
   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化
   PCなどからIoTなどへ
4. 攻撃者の多様化・高度化
   犯罪組織の高度化
   国家を後ろ盾とした攻撃の増加

攻撃者と攻撃目的

大分類	分類	目的	備考
個人	攻撃初心者	興味本位	既存のツールを利用
	職業的攻撃者	金銭・名誉	攻撃が発覚しにくいツール
攻撃者団体	テロリスト	社会的混乱	職業的攻撃者との結合も
	犯罪組織	金銭	組織化・高度化 犯罪者にツールを売るビジネスも
国またはそれに準ずる組織		国益	教育機関を持つ 金銭的余裕がある 未発表の脆弱性をつくことも

谷口星彦「攻撃者の分類の一考察」日本セキュリティ・マネジメント学会誌，第31巻，第2号　pp17-22　(2017)などを参照し作成

Verizon2018年データ漏洩・侵害調査報告書

サイバー攻撃の目的

金銭入手:　攻撃の76%

スパイ活動:　20%弱

愉快犯:　10%弱

2020年度の報告書では86%

攻撃者

サイバー犯罪は、麻薬売買などと並んでわりのよい犯罪だと言われている。

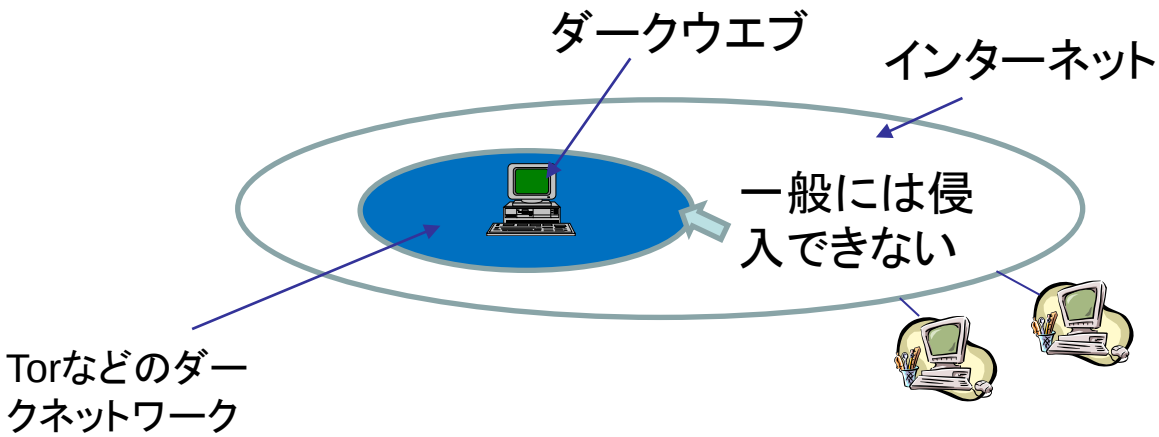
「先進的サイバー犯罪組織には、最高経営責任者や最高情報責任者だけでなく研究開発を行う部門やコンピュータウイルスの品質保証を行う部門もあるという衝撃的事実も紹介されている。」[1]

攻撃側の分化（攻撃依頼者、攻撃実行者、攻撃ツール提供者、コーディネータ）

ダークウェブとは

ダークウェブ(Dark web)はTor（“The Onion Router”）やI2P("Invisible Internet Project")などを用いたダークネット(インターネットを使用するが、アクセスするために特定のソフトウェア、設定、認証が必要なオーバーレイ・ネットワーク)に存在するWorld Wide Webコンテンツ

Wikipediaより



ダークWEBのサービスの例

1. ボットネットへの指示
2. ビットコインサービス（マネーロンダリング）
3. ダークマーケット（違法薬物、個人情報、拳銃、臓器売買、人身売買など）
4. ハッキングサービス
5. 詐欺（偽サイト）

Wikipediaなどより

FBI　中国籍の2人を起訴

WANTED BY THE FBI

CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Unauthorized Access; Conspiracy to Access Without Authorization and Damage Computers; Conspiracy to Commit Theft of Trade Secrets; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

Li Xiaoyu　　Dong Jiazhi

CAUTION

On July 7, 2020, a grand jury in the United States District Court for the Eastern District of Washington indicted Li Xiaoyu and Dong Jiazhi for their alleged participation in a long-running campaign of computer network operations targeting the networks of United States and foreign companies across a wide variety of industries, including high tech manufacturing; civil, heavy, and medical device engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense. The indictment highlighted Li and Dong's alleged actions, including a recent focus on COVID-19 research, testing, and treatment; the targeting of political dissidents, religious minorities, and human rights advocates in mainland China, Hong Kong, the United States, and Canada; and the intrusions into corporate networks of countries in Europe and Asia.

Some of Li and Dong's network operations were allegedly undertaken for their own economic benefits, while others were allegedly for the benefits of China's Ministry of State Security (MSS), including the Guangdong State Security Department.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Seattle

国際手配

10年以上にわたり米国内外の企業にハッキングを仕掛け、情報を盗んだとして、米司法省は21日、中国籍の男性ハッカー2人を企業秘密の窃盗など11の罪で起訴したと発表した。被害額は数億ドル（数百億円）相当に上り、日本企業も標的になっていたという。

7日に西部ワシントン州の連邦大陪審によって正式起訴されたのは、李嘯宇（34）と董家志（33）の両容疑者。

日本関連では、ゲームソフトのソースコード▽高性能ガスタービンの図面や仕様書▽医療機器のデザインデータなどが狙われたとされる。

https://www.msn.com/ja-jp/news/world/%E6%97%A5%E6%9C%AC%E4%BC%81%E6%A5%AD%E3%82%82%E3%83%8F%E3%83%83%E3%82%AD%E3%83%B3%E3%82%B0%E8%A2%AB%E5%AE%B3%E3%81%8B-%E7%B1%B3-%E4%B8%AD%E5%9B%BD%E7%B1%8D%E3%81%AE2%E4%BA%BA%E3%82%92%E8%B5%B7%E8%A8%B4/ar-BB170qGT?ocid=msedgdhp

イスラエル軍、イスラム過激派のサイバー部隊に空爆実施

イスラエル軍が、イスラム過激派組織ハマスによるサイバー攻撃を阻止し、そのサイバー部隊のアジトと目されるガザ地区の建物への空爆を実施しました。

ハマスが行おうとしたとされるサイバー攻撃に対してほぼリアルタイムで物理的な反撃を加え、その能力を壊滅させるものでした。

サイバー戦から
物理的戦争へ

https://japanese.engadget.com/2019/05/07/israel-responds-to-cyberattack/

目次

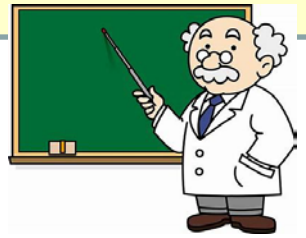
1. 中小企業におけるセキュリティ対策の現状
2. セキュリティの基礎
3. サイバー攻撃の動向
4. 中小企業のためのセキュリティガイド
5. おわりに

セキュリティガイドライン

種々のセキュリティガイドラインが

① 経営者向け:「サイバーセキュリティ経営ガイドライン第2版」 2017（経済産業省/情報処理推進機構）

② 中小企業向け:「中小企業の情報セキュリティ対策ガイドライン第3版」 2019 （情報処理推進機構）



中小企業の情報セキュリティ対策ガイドライン第3版の概要（1）

構　成		概　要
本編	第１部　経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
本編	第２部　実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付録	付録１　情報セキュリティ５か条	組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。
付録	付録２　情報セキュリティ基本方針（サンプル）	組織としての情報セキュリティに対する基本方針書のサンプルです。
付録	付録３　５分でできる！情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
付録	付録４　情報セキュリティハンドブック（ひな形）	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
付録	付録５　情報セキュリティ関連規程（サンプル）	情報セキュリティに関する社内規則を文書化したもののサンプルです。
付録	付録６　中小企業のためのクラウドサービス安全利用の手引き	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
付録	付録７　リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。

https://www.ipa.go.jp/files/000055520.pdf

経営者の皆様へ

1. 情報セキュリティ対策は、経営に大きな影響を与えます！

2. 対策の不備により経営者が法的・道義的責任を問われます！

3. 組織として対策するために、担当者への指示が必要です！

https://www.ipa.go.jp/files/000055520.pdf

対策を怠ることで企業が被る不利益

① 金銭損失：ウイルス感染で数日間業務が停止し、数千万の損失、損害賠償など

② 顧客の喪失：顧客情報の流出によるの信頼の失墜など

③ 業務の停滞：業務システム事故による、インターネット遮断がもたらす業務停滞など

④ 従業員の影響：従業員のみを罰して管理職が責任を取らないことによる従業員の働く意欲の低下など

https://www.ipa.go.jp/files/000055520.pdf

経営者の皆様へ

1. 情報セキュリティ対策は、経営に大きな影響を与えます！

2. 対策の不備により経営者が法的・道義的責任を問われます！

3. 組織として対策するために、担当者への指示が必要です！

https://www.ipa.go.jp/files/000055520.pdf

経営者が負う責任

① 経営者が問われる法的責任

個人情報保護法

マイナンバー法

不当競争防止法

金融商品取引法

民法など

② 関係者や社会に対する責任

会社役員が、会社法上の責任をとわれる可能性

https://www.ipa.go.jp/files/000055520.pdf

経営者が認識すべき3原則

原則１：情報セキュリティ対策は経営者のリーダシップで進める

原則２：委託先の情報セキュリティ対策まで考慮する

原則３：関係者（顧客、取引先、委託先、代理店、利用者、株主など）とは常に情報セキュリティに関するコミュニケーションをとる

https://www.ipa.go.jp/files/000055520.pdf

中小企業で実行すべき「重要7項目の取り組み」

1. 情報セキュリティに対する組織全体の対応方針を決める
2. 情報セキュリティ対策のための予算や人材を確保する
3. 必要と考えられる対策を検討させて実行を指示する
4. 情報セキュリティ対策に関する適宜の見直しを指示する
5. 緊急時の対応や復旧のための体制を整備する
6. 委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
7. 情報セキュリティに関する最新動向を収集する

https://www.ipa.go.jp/files/000055520.pdf

中小企業における対応法

ステップ1：まず始めましょう

「情報セキュリティ5か条」を社内で配布するなどまずできるところから実施

ステップ2：現状を知り改善しましょう

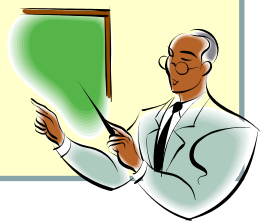
「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成、「5分でできる自社診断」の実施、「情報セキュリティハンドブック（ひな形）」を参考に具体的対策を定め、従業員に周知など

ステップ3：本格的に取り組みましょう

情報セキュリティ管理体制を構築し予算を確保、対応すべきリスクと対策を考慮し、「情報セキュリティ関連規定（サンプル）」を参考に、規定を作成、委託時に必要な対策の検討など

ステップ4：改善を続けよう

「より強固にするするための方策」を参考にし自社向け対策を強化



https://www.ipa.go.jp/files/000055520.pdf

情報セキュリティ5か条

1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！

https://www.ipa.go.jp/files/000055520.pdf

中小企業における対応法

ステップ１：まず始めましょう

「情報セキュリティ5か条」を社内で配布するなどまずできるところから実施

ステップ２：現状を知り改善しましょう

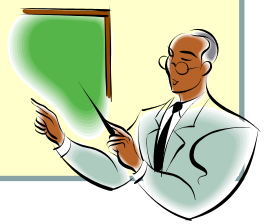
「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成、「5分でできる自社診断」の実施、「情報セキュリティハンドブック（ひな形）」を参考に具体的対策を定め、従業員に周知など

ステップ３：本格的に取り組みましょう

情報セキュリティ管理体制を構築し予算を確保、対応すべきリスクと対策を考慮し、「情報セキュリティ関連規定（サンプル）」を参考に、規定を作成、委託時に必要な対策の検討など

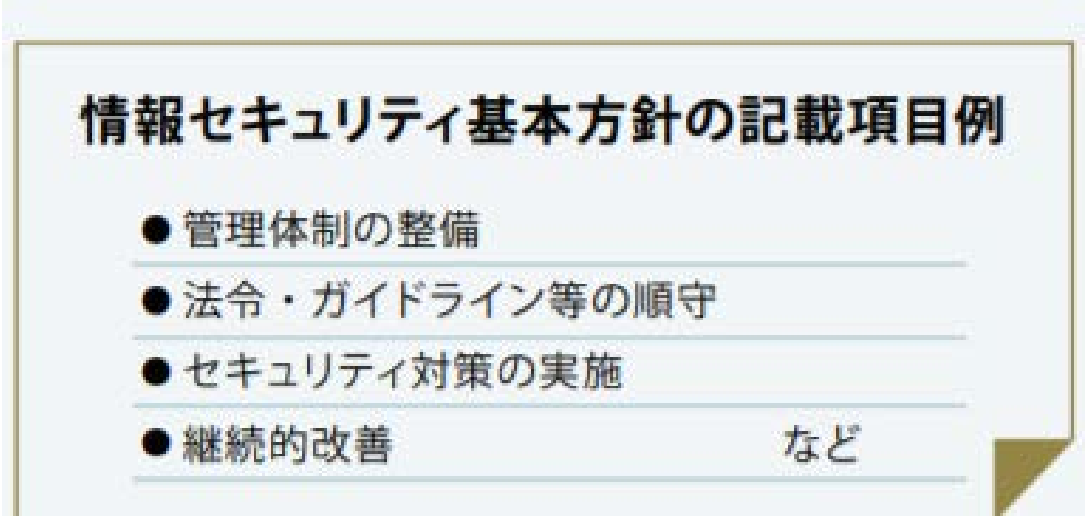
ステップ４：改善を続けよう

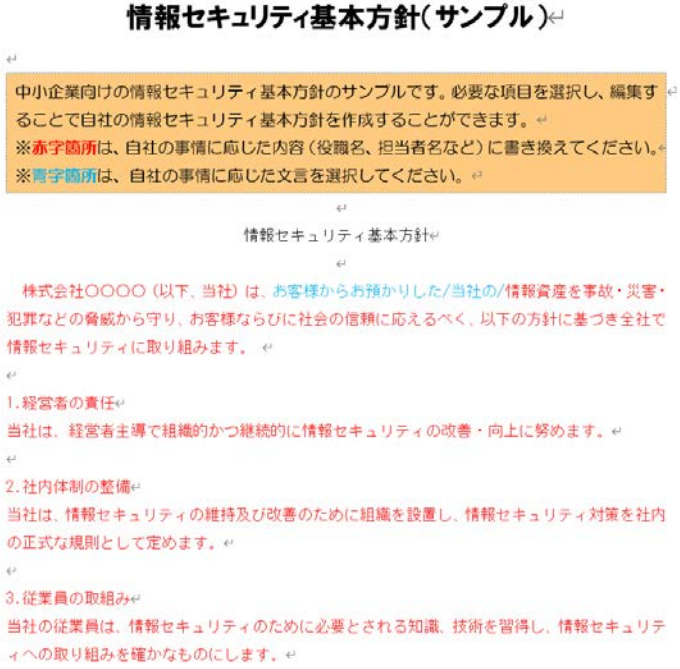
「より強固にするするための方策」を参考にし自社向け対策を強化



https://www.ipa.go.jp/files/000055520.pdf

情報セキュリティ基本方針の作成と周知





情報セキュリティ基本方針（サンプル）

中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。
※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。
※青字箇所は、自社の事情に応じた文言を選択してください。

情報セキュリティ基本方針

株式会社○○○○（以下、当社）は、お客様からお預かりした/当社の/情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1.経営者の責任
当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2.社内体制の整備
当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

3.従業員の取組み
当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

https://www.ipa.go.jp/files/000055520.pdf

5分でできる情報セキュリティ自社診断（1）

実施状況の把握

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	−1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	−1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	−1
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	−1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	−1

https://www.ipa.go.jp/files/000055520.pdf

5分でできる情報セキュリティ自社診断（2）

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？	4	2	0	−1
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	−1
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	−1
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	−1
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	−1
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	−1
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？	4	2	0	−1
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	−1
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	−1
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	−1
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	−1
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	−1
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	−1

https://www.ipa.go.jp/files/000055520.pdf

5分でできる情報セキュリティ自社診断（3）

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	−1
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	−1
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	−1
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	−1
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	−1
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	−1
	25	情報セキュリティ対策（上記１～24など）をルール化し、従業員に明示していますか？	4	2	0	−1

https://www.ipa.go.jp/files/000055520.pdf

Security Action

「SECURITY ACTION」は中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度です。「5分でできる！情報セキュリティ自社診断」を実施し、「情報セキュリティ基本方針」を定め、公開することで２段階目の「二つ星」を使用することができます。

Check!!
☑ 5分でできる！
情報セキュリティ自社診断

Check!!
☑ 情報セキュリティポリシー
（基本方針）

セキュリティ対策自己宣言

SECURITY ACTION 二つ星
https://www.ipa.go.jp/security/security-action/

https://www.ipa.go.jp/files/000055520.pdf

対策の決定と周知

https://www.ipa.go.jp/files/000055520.pdf

中小企業における対応法

ステップ１：まず始めましょう

「情報セキュリティ5か条」を社内で配布するなどまずできるところから実施

ステップ２：現状を知り改善しましょう

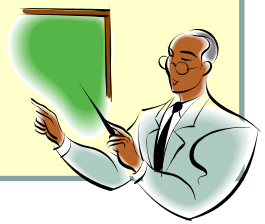
「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成、「5分でできる自社診断」の実施、「情報セキュリティハンドブック（ひな形）」を参考に具体的対策を定め、従業員に周知など

ステップ３：本格的に取り組みましょう

情報セキュリティ管理体制を構築し予算を確保、対応すべきリスクと対策を考慮し、「情報セキュリティ関連規定（サンプル）」を参考に、規定を作成、委託時に必要な対策の検討など

ステップ４：改善を続けよう

「より強固にするするための方策」を参考にし自社向け対策を強化



https://www.ipa.go.jp/files/000055520.pdf

情報セキュリティ関連規定（サンプル）

https://www.ipa.go.jp/files/000055520.pdf

役割と責任分担

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	情報セキュリティ対策のためのシステム管理を行います。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	情報セキュリティ対策が適切に実施されているか点検します。

https://www.ipa.go.jp/files/000055520.pdf

中小企業における対応法

ステップ１：まず始めましょう

「情報セキュリティ5か条」を社内で配布するなどまずできるところから実施

ステップ２：現状を知り改善しましょう

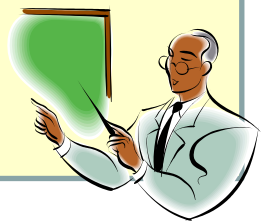
「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成、「5分でできる自社診断」の実施、「情報セキュリティハンドブック（ひな形）」を参考に具体的対策を定め、従業員に周知など

ステップ３：本格的に取り組みましょう

情報セキュリティ管理体制を構築し予算を確保、対応すべきリスクと対策を考慮し、「情報セキュリティ関連規定（サンプル）」を参考に、規定を作成、委託時に必要な対策の検討など

ステップ４：改善を続けよう

「より強固にするするための方策」を参考にし自社向け対策を強化



https://www.ipa.go.jp/files/000055520.pdf

より強固にするための方策

(1)情報収集と共有

情報セキュリティに関する情報収集の方法と情報共有の枠組みについて説明します。

(2)ウェブサイトの情報セキュリティ

ウェブサイトを安全に構築し、運用するためのポイントを説明します。

(3)クラウドサービスの情報セキュリティ

クラウドサービスを安全に利用するためのポイントを説明します。

(4)セキュリティサービス例と活用

情報セキュリティに関する外部サービスを説明します。

(5)技術的対策例と活用

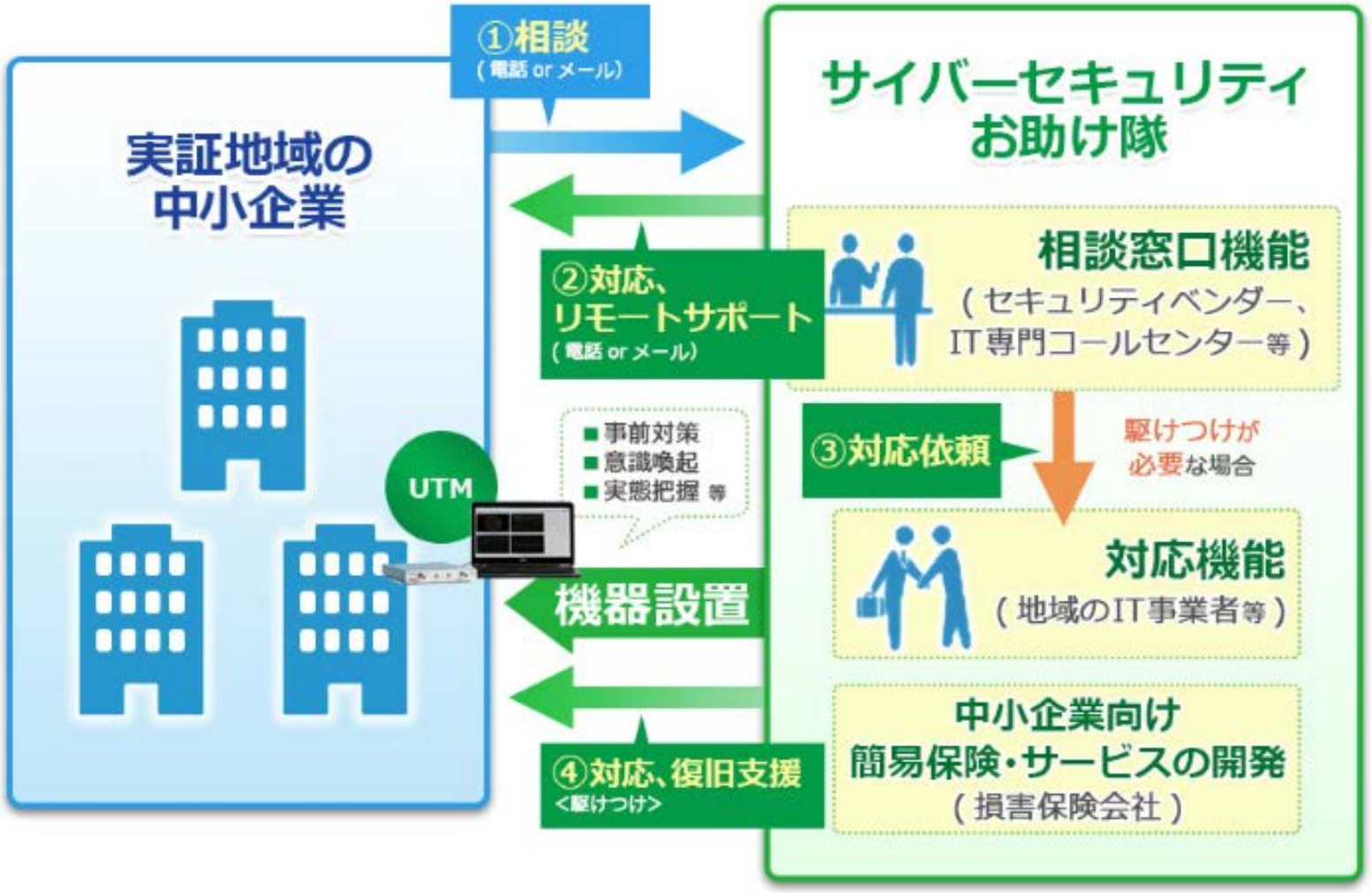
ITを活用する際の技術的対策について説明します。

(6)詳細リスク分析の実施方法

「リスク分析シート」(付録7)を活用した詳細リスク分析の実施方法を説明します。

https://www.ipa.go.jp/files/000055520.pdf

サイバーセキュリティお助け隊のイメージ



https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

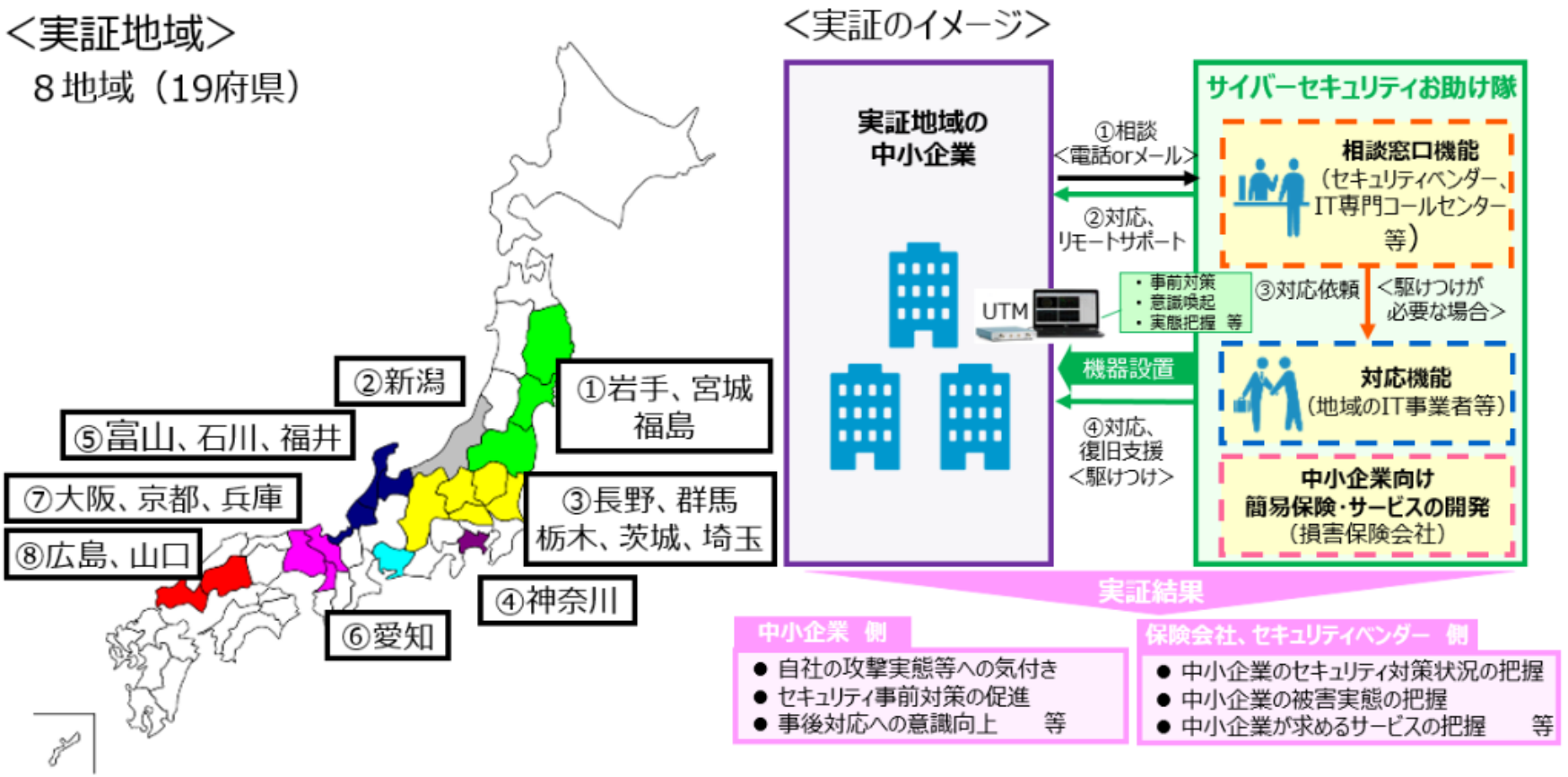
UTM製品

UTM（Unified Threat Management）アプライアンスにはファイアウォールやVPN、コンピュータウイルス対策、不正侵入検知・防御（IDS/IPS）、Webコンテンツフィルタリングといったネットワークセキュリティに必要な一通りの機能が実装されている。

PC接続10-30台程度
価格20万程度、月額数千円程度

https://special.oaland.jp/security/?gclid=EAIaIQobChMIhamehJTi6gIVTdeWCh37YQqPEAAYAiAAEgI17vD_BwE

IPA主催のサイバーセキュリティお助け隊実証実験（2019）



https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html

セキュリティ機器等による サイバー攻撃の実態把握

事業主体	実証参加企業数	セキュリティ機器等によるサイバー攻撃の実態把握		
		(設置数)	内訳	社数
①株式会社デジタルハーツ	111	81	ネットワークセンサー	81
②東日本電信電話株式会社	148	148	UTM機器	148
③富士ゼロックス株式会社	112	101	UTM機器	101
④SOMPOリスクマネジメント株式会社	150	110	UTM機器	38
			クラウド型WAF	0
			EDRソフト	72
⑤株式会社PFU	120	97	PC脅威検知ツール	97
⑥MS&ADインターリスク総研株式会社	201	55	据置型UTM	27
			クラウド型UTM	28
⑦大阪商工会議所	112	112	UTM機器	112
⑧株式会社日立製作所	110	23	UTM機器	10
			EDRソフト	13
計	**1,064**	**727**		

https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html

対応状況

<コールセンター対応及びインシデント対応等の状況>

対応種別	総数	相談・インシデント等対応状況	発生件数
コールセンター対応	741件	実証参加に関する問合せ	64件
		セキュリティ機器設置等の問合せ	432件
		セキュリティ対応の相談	113件
		その他	132件
インシデント等対応	**128件**	**電話及びリモートによるインシデント対応 ※**	**110件**
		訪問によるインシデント対応（駆け付け対応）	**18件**
その他訪問対応	68件	機器設置等のトラブル対応	19件
		その他（セキュリティ機器の導入・設置支援等）	49件

※電話およびリモートによるインシデント対応には、訪問によるインシデント対応の一次対応を含む

https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html

全体まとめ

中小企業のセキュリティ状況等の実態

◆業種や規模を問わず、内外に向けた不正通信等を数多く検知
◆計128件のインシデントが発生し、うち駆け付け対応を18件実施
◆サイバー攻撃を検知及び防御できるUTM機器等の導入は2割強のみ
◆約7割の企業においては社内のセキュリティ体制構築ができていない
◆サイバー保険の認知度は低く、普及が進んでいない

対策普及に向けた取組みの方向性

◆セキュリティ対策への理解を促す継続的な意識啓発
◆導入・運用しやすいUTM等セキュリティ機器の開発及び普及促進
◆セキュリティ機器と専門家による伴走型支援のワンパッケージ化を検討
◆中小企業に求められる支援サービスのスリム化によるコストの低廉化
◆加入しやすいサイバー保険の開発と普及促進

取組み推進のポイント

◆地域特性や産業特性等を十分に考慮し、セキュリティ関連のみならず地域コミュニティを形成する様々な企業、機関、団体等との連携が有効

◆実証サービスのビジネス化を促すため、事業主体等がコンソーシアムを形成するなど、今後のビジネス化に向けた必要な情報共有や検討を実施することができる仕組みの構築が有効

https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai_houkoku.html

目次

終りに

- サイバー攻撃は今後も厳しくなる。
- 適切なサイバーセキュリティ対策をやり続けるしかない。
- サイバーセキュリティ対策は経営者の責任とみなされる時代に。

参考情報源

セキュリティ情報リンク集

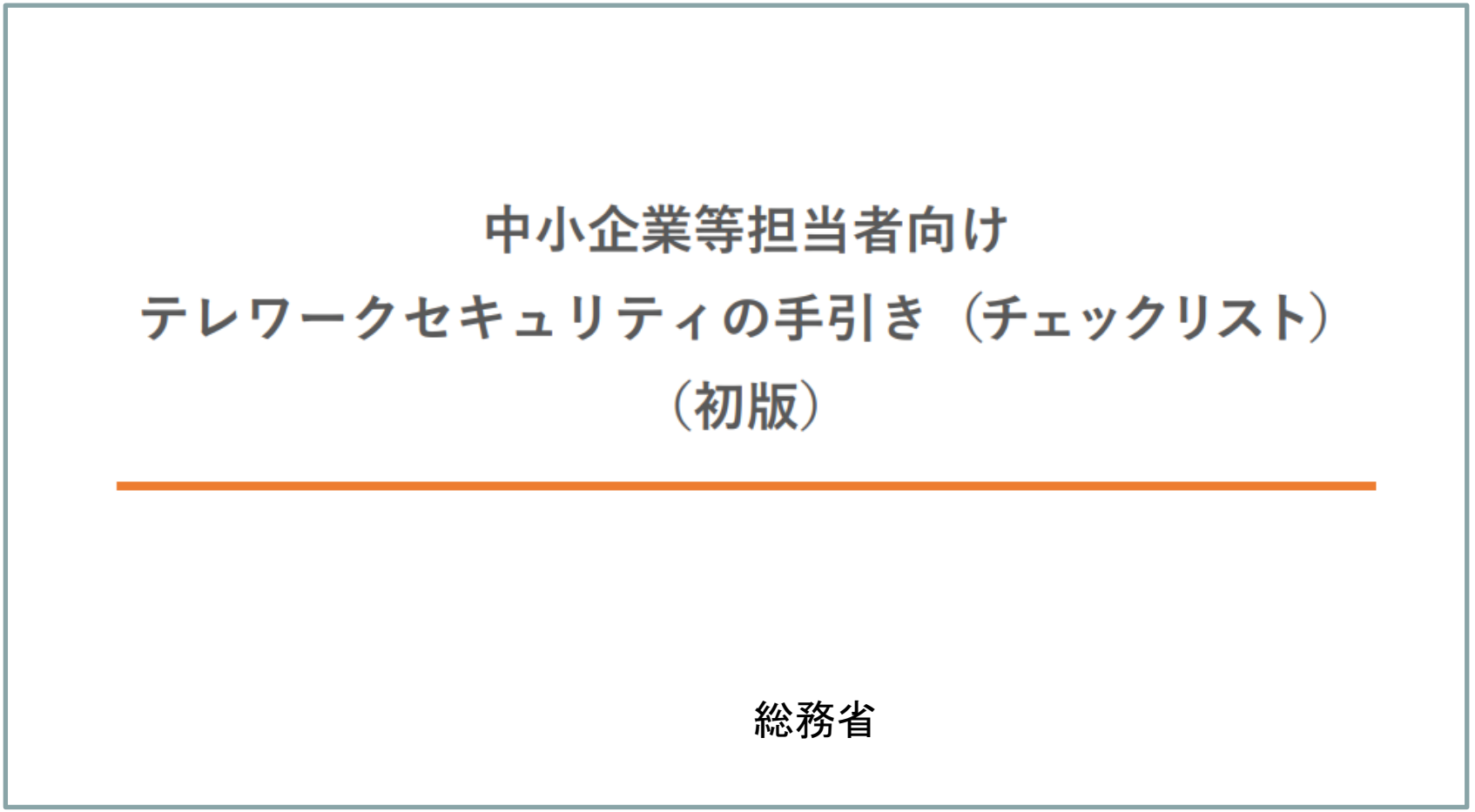
1）情報処理推進機構(IPA)のセキュリティ関連情報
http://www.ipa.go.jp/

2）警察庁サイバー犯罪対策
http://www.npa.go.jp/cyber/index.html

3）内閣サイバーセキュリティセンター
http://www.nisc.go.jp/

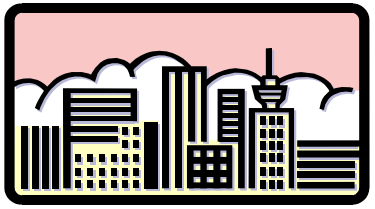
4）JPCERT　http://www.jpcert.or.jp/

こんなのもあります。



https://www.soumu.go.jp/main_content/000706649.pdf

学会関連

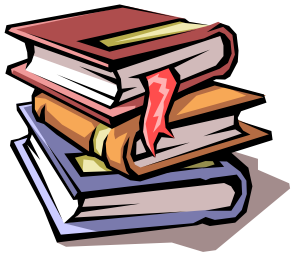


分類	名称	頻度	備考
国内	ｺﾝﾋﾟｭｰﾀｾｷｭﾘﾃｨ研究会（情報処理学会）	年4回	H10年発足、他にシンポジウムCSS
	情報ｾｷｭﾘﾃｨ研究会（電子情報通信学会）	年6回	暗号中心。他に年1回のシンポジウム（SCIS）
	日本ｾｷｭﾘﾃｨﾏﾈｰｼﾞﾒﾝﾄ学会全国大会	年1回	セキュリティ管理、セキュリティ監査、評価等
国際	CRYPTO,EUROCRYPT (IACR*主催)	年1回	世界最大級の暗号学会
	Security and Privacy(IEEE) SEC （IFIP主催）	年1回	システムセキュリティ関連
	USENIX NDSS	年1回	ネットワークセキュリティ関連

*IACR:International Association for Cryptologic Research

参考文献

1） 佐々木良一監修「情報セキュリティの基礎」共立出版、2011
２）中島明日香「サイバー攻撃」講談社　ブルーバックス、2018
３）佐々木良一「ITリスクの考え方」岩波新書、2008
４）佐々木良一編著「ITリスク学　情報セキュリティを超えて」共立出版、2013
５）佐々木良一編著「デジタル･フォレンジックの基礎と実践」電大出版、2017年3月出版
６）伊東寛「サイバー・インテリジェンス」祥伝社，2015




END